CONSULTORÍA APLICADA AL PROCESO DE TECNOLOGÍA DE LA INFORMACIÓN DE LA EMPRESA CONGLOMERADO TÉCNICO COLOMBIANO S.A. – CONTECSA S.A.

ANA MARIA MOLINARES DONADO
LENYS RANGEL FERRER
MANUELA MARIA VILLAR ÁVILA

UNIVERSIDAD DE LA COSTA CUC
ESPECIALIZACIÓN EN AUDITORIA A LOS SISTEMAS DE INFORMACIÓN
DEPARTAMENTO DE POSTGRADO

BARRANQUILLA
2014

CONSULTORÍA APLICADA AL PROCESO DE TECNOLOGÍA DE LA INFORMACIÓN DE LA EMPRESA CONGLOMERADO TÉCNICO COLOMBIANO S.A. – CONTECSA S.A.

ANA MARIA MOLINARES DONADO
LENYS RANGEL FERRER
MANUELA MARIA VILLAR ÁVILA

Trabajo de Grado

Asesor: Ing. Telma Barraza Olaya
Especialista en Auditoria de Sistemas

UNIVERSIDAD DE LA COSTA CUC
ESPECIALIZACIÓN EN AUDITORIA A LOS SISTEMAS DE INFORMACIÓN
DEPARTAMENTO DE POSTGRADO

BARRANQUILLA
2014

Nota de Aceptación:

Presidente del Jurado

Jurado

Jurado

Barranquilla, Octubre 15 de 2014

DEDICATORIA

Dedico especialmente este trabajo a Dios, por ser Él mi creador, porque Su presencia y guía, ha conllevado a la culminación en buen término de todos los planes que me he propuesto a lo largo de mi vida.

A mi primogénita, mi madre y al padre de mi hija, personas importantes para mí y a quienes amo profundamente, principalmente a Paula, porque quiero sembrar en su corazón la premisa de que siempre hay que trabajar y esforzarse por ser mejor cada día.

Finalmente -y no menos importante-, a todas aquellas personas que cada día han estado ahí estimulándome, a través de su cariño, su confianza, apoyo y dirección, aquellos, a los que siempre he considerado instrumentos de Dios para bendecir para mi vida.

"Sólo hay un camino que conduce al éxito y está constituido de esfuerzo y persistencia. Pero los únicos esfuerzos que pueden exigir todas nuestras energías son aquellos que realmente merecen la pena"

Dr. Robert Jarvik

Ana María Molinares Donado

DEDICATORIA

Cada persona tiene sus metas y sus ideales que con esfuerzos son logrados. Hoy agradezco a Dios por permitirme cumplir uno de ellos, por darme la sabiduría y la guía necesaria en el caminar de la vida.

A mis padres Arnedo y Yaneth, por ser ellos un apoyo fundamental en cada uno de mis objetivos, por brindarme su confianza, sus principios, sus valores. Gracias a ellos soy quien soy en el presente.

A mis hermanos Jovannis y Shirley por ser personas incondicionales, por estar pendiente de los pequeños detalles.

A mi novio Luis por su compresión, por darme el espacio suficiente, y darme una voz de aliento en la culminación de estudios y en el desarrollo de la tesis.

A nuestra tutora Ingeniera Telma Barraza por ser nuestra ayuda, nuestra guía ejemplar, por brindarnos sus conocimientos, su experiencia profesional y ser persistente en nuestra tesis.

A Ana molinares que fue mi compañera durante la travesía de estudio en la especialización; hoy es mi amiga y consejera en el presente. Gracias por ser tan constante.

"Nuestra recompensa se encuentra en el esfuerzo y no en el resultado. Un esfuerzo total es una victoria completa".

Mahatma Gandhi

Lenys Rangel Ferrer

DEDICATORIA

Al tomar la decisión de empezar esta especialización, tenía claro mis ganas de aprender y luego ponerlo en práctica en mi trabajo. Primeramente quiero dedicarle a Dios quién supo guiarme por el buen camino, darme fuerzas para seguir adelante y no desmayar en los problemas que se me presentaban, enseñándome a encarar las adversidades sin perder nunca la dignidad ni desfallecer en el intento.

A mi madre, por su apoyo y amor incondicional. A mis hermanos por estar siempre presentes en todo momento de mi vida. A mis sobrinos que son mis grandes tesoros y a mi hija que es mi motivación, inspiración y felicidad.

"La dicha de la vida consiste en tener siempre algo que hacer, alguien a quien amar y alguna cosa que esperar".
Thomas Chalmers.

Manuela Maria Villar Ávila

AGRADECIMIENTOS

Principalmente nuestro más sincero agradecimiento a Dios por ser el creador de la vida y de nuestra motivación para culminar esta meta.

Al personal docente que labora en la Universidad de la Costa, por brindarnos una excelente formación profesional durante el desarrollo de esta Especialización.

A la Ingeniera Telma Barraza, por su valioso apoyo y conducción a través de la asesoría en este trabajo especial de Grado.

Finalmente, a todas las personas que con su colaboración y apoyo, participaron en la realización de este gran sueño, en especial, al grupo de trabajo de CONTECSA S.A., que nos permitió demostrar nuestros conocimientos y habilidades.

RESUMEN

El presente trabajo tiene como fundamento reflejar el desarrollo de una consultoría, aplicada a la investigación y análisis sobre las actividades relacionadas con la administración y funcionamiento del proceso de TI en la empresa CONTECSA S.A., (empresa dedicada a la ejecución de consultoría y/o construcción de obra civil), con miras a generar una propuesta de mejora para el mismo.

En la primera etapa, se recolectó información en general, para entender el entorno y la situación actual de las actividades TI en la organización. En la segunda etapa, se presenta el diagnóstico sustentado en los resultados de entrevistas y pruebas aplicadas. Esta investigación es de tipo descriptiva y se vincula a un proyecto factible, por lo tanto, es una propuesta de mejora, de tal manera que los resultados obtenidos permitieron proponer una serie de recomendaciones aplicables al uso de las TI en la empresa. A través de unos informes que sugieren el uso eficiente y a la medida de los recursos de TI disponibles en la empresa, asimismo, medir y clasificar los riesgos asociados con miras a reducirlos.

Palabras Claves

- Amenazas
- Riesgo
- Seguridad de la Información
- Sistemas de Información

ABSTRACT

This work is based reflect the development of a consultancy, applied research and analysis activities related to the administration and operation of the process of IT in the company CONTECSA S.A., (a company dedicated to the execution of consulting and/or construction civil works), in order to generate a proposal to improve it.

In the first stage, collected generaly information to understand the environment and the current status of IT activities in the organization. In the second step, the diagnostic, supported interview results and evidence is presented applied. This research is descriptive and is linked to a feasible project, therefore, is a proposed improvement, so that the obtained results allowed to propose a series of recommendations on the use of IT in the company. Through some reports suggesting the efficient use and tailored IT resources available in the enterprise also measure and rank the risks in order to reduce them.

Key Words

- Information Security
- Information Systems
- Threats
- Risk

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

INTRODUCCIÓN

Hacer las cosas bien en las Tecnologías de la Información (TI) es fácil si las organizaciones se apoyan en un conjunto de buenas prácticas que permitan trabajar con agilidad y efectividad. Independientemente de que las TI sean o no la base del modelo de negocios de una determinada empresa, lo cierto es que hoy día éstas son cada vez más dependientes de ellas, para soportar y mejorar el desempeño de sus procesos misionales y así, poder satisfacer, de mejor manera, las necesidades tanto del cliente interno como externo.

Cada una de las actividades relacionadas con TI deben estar ejecutadas bajo criterios que aseguren que este proceso proporcione un valor y entregue los servicios de forma consistente. La aplicación de un conjunto de buenas prácticas permite que la gestión de TI en una organización trabaje en un punto de equilibrio entre la óptima calidad y un costo adecuado.

Esta Consultoría apunta, principalmente, a evaluar y definir el nivel en que se encuentra el proceso de Tecnología de la Información en la empresa Conglomerado Técnico Colombiano S.A. - CONTECSA S.A., de tal forma que ello permita la identificación objetiva de los riesgos que afecten la calidad e integridad de la información y de su infraestructura tecnológica actual. Las recomendaciones u observaciones, coadyuvarán a la alta gerencia en la toma de decisiones estratégicas que mejoren el desempeño de las TI en la organización, y en general, el desempeño de los demás procesos que se apoyan en éste, generando un impacto positivo sobre el desempeño global de la organización, sobre su imagen corporativa y especialmente, ante sus clientes.

1. INFORMACIÓN GENERAL DEL PROYECTO

Título	**Consultoría Aplicada al Proceso de Tecnología de la Información de la Empresa Conglomerado Técnico Colombiano S.A. – Contecsa S.A.**
Delimitación	Infraestructura Tecnológica y la aplicación SICON
Tipo de Empresa	Privada – Consultoría y Ejecución de Obras Civiles
Desarrollado por	Ing. Ana María Molinares Donado - **amolinares@gmail.com** Ing. Lenys Rangel Ferrer - **lensyran@gmail.com** Ing. Manuela Villar Ávila – **ingmanuelavillar@gmail.com**
Facultad	Postgrado – Auditoria a los Sistemas de Información
Tipo de Proyecto	Investigación de Campo, Descriptiva y Documental
Duración del Proyecto	Seis (6) Meses

2. PLANTEAMIENTO DEL PROBLEMA

Hoy día, las exigencias de los clientes constituyen un factor clave y relevante para el éxito de toda organización. Aplicar un sistema de Gestión de la Calidad constituye una gran ventaja competitiva a la hora de garantizar una buena gestión. Es por esto por lo que la alta gerencia de CONTECSA S.A., decidió implementar un sistema de calidad. Para tal efecto, es prioridad cumplir con los lineamientos que el sistema como tal exige, de manera tal que se viabilice el alcance del logro de los objetivos estratégicos establecidos, fortaleciendo y mejorando su desempeño.

En medio de todo este frenesí de calidad e identificación de procesos, surgió la necesidad de evaluar objetivamente cómo se desarrolla en CONTECSA actualmente la gestión en los temas relacionados en tecnología de la información y el desarrollo de aplicaciones que optimizan las actividades misionales. A partir de ello, surgió la necesidad de evaluar este proceso y nació la oportunidad de realizar esta Consultoría, cuyo resultado brindará un análisis sobre la situación actual de la gestión de tecnología de la información, una evaluación de la eficacia y eficiencia en sus procesos de TI con base en unos marcos de referencia establecidos. Por supuesto que se formularán las recomendaciones pertinentes, con el ánimo de contribuir a la optimización del uso de sus recursos y de manera general, a su plan de mejoramiento continuo.

3. JUSTIFICACIÓN

La contribución que representará la información resultado de la investigación y las recomendaciones que se consignarán en esta Consultoría, serán un aporte particularmente útil y significativo al plan de mejoramiento de la calidad que se está implementando en CONTECSA S.A., debido a que su desarrollo descriptivo, estará orientado para que sirva de apoyo a la gestión administrativa y de control. Los resultados de esta evaluación serán una alternativa-base desde una perspectiva diferente y las recomendaciones apuntarán a la utilización óptima de los recursos, además de enfatizar la relevancia en la aplicación de un ambiente y políticas de control adecuados.

Mediante la aplicación de esta consultoría, la empresa CONTECSA S.A., contará con una evaluación precisa de su proceso de TI. Adicionalmente, permite adquirir y validar experiencia calificada al emplear los conocimientos teórico-prácticos y las técnicas asimiladas durante la participación en la Especialización en Auditoría a los Sistemas de Información y optar por este título académico.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Realizar una Consultoría a la empresa **CONGLOMERADO TÉCNICO COLOMBIANO S.A. –CONTECSA S.A.,** específicamente a sus sistemas de información e infraestructura tecnológica, basándonos en los estándares de buenas prácticas como COBIT® 4.1, ISO 27001, ISO 27005 e ITIL® V3.

4.2 OBJETIVOS ESPECÍFICOS

- ✓ Evaluar la infraestructura tecnológica actualmente implementada para el manejo de la información.
- ✓ Identificar posibles riesgos asociados a los procesos que atenten en contra del logro de los objetivos del negocio y de la seguridad de la información.
- ✓ Determinar el nivel de madurez de los procesos, utilizando como apoyo el marco de referencia COBIT®.
- ✓ Identificar y evaluar los controles existentes para los procesos seleccionados
- ✓ Verificar la confidencialidad, la disponibilidad, la integridad y el procesamiento de la información. Asimismo, las herramientas tecnológicas en uso.
- ✓ Formular recomendaciones en pro de fortalecer y optimizar los sistemas actualmente implementados.
- ✓ Analizar la asignación y el uso actual de los recursos.

5. MARCO DE REFERENCIA

Este capítulo describe términos y/o conceptos claves que se emplearon a lo largo de esta Consultoría, asimismo, el entorno legal aplicado al objeto social de la empresa. Estas definiciones son el resultado de indagaciones a diversas fuentes bibliográficas y páginas web de instituciones gubernamentales y privadas, y apreciaciones resultado de la participación en la Especialización. Es válido aclarar que la mayoría de estas definiciones fueron modificadas con el objeto de enfatizar en la comprensión de la misma.

5.1 MARCO TEÓRICO

5.1.1 COBIT® (Control Objectives for Information Related Technology).

Las siglas COBIT® significan Objetivos de Control para Tecnología de Información y Tecnologías relacionadas. El modelo fue creado por la Asociación para la Auditoría y Control de Sistemas de Información, (ISACA®, en inglés: Information Systems Audit and Control Association) y promovido por el Instituto de Administración de las Tecnologías de la Información (ITGI, en inglés: IT Governance Institute) en 1992. Este instituto provee un estándar que generalmente es aplicado y aceptado en buenas prácticas de seguridad de TI, con el fin de apoyar las necesidades gerenciales en cuanto a monitoreo de los niveles apropiados de seguridad de TI que se deben seguir en las organizaciones[1].

La primera edición fue publicada en 1996; la segunda edición en 1998; la tercera edición en 2000 (la edición on-line estuvo disponible en 2003); y la cuarta edición en diciembre de 2005, y la versión 4.1 está disponible desde mayo de 2007.

[1] *http://www.inteco.es/glossary/Formacion/Glosario/COBIT*

En su cuarta edición, COBIT® tiene 34 objetivos de alto nivel que cubren 210 objetivos de control (específicos o detallados) clasificados en cuatro dominios: Planificación y Organización, Adquisición e Implementación, Entrega y Soporte, y, Supervisión y Evaluación en inglés: Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate.

5.1.1.1 **Misión.**

La misión de COBIT® es "investigar, desarrollar, publicar y promocionar un conjunto de objetivos de control generalmente aceptados para las tecnologías de la información que sean autorizados (dados por alguien con autoridad), actualizados, e internacionales para el uso del día a día de los gestores de negocios (también directivos) y auditores." Gestores, auditores, y usuarios se benefician del desarrollo de COBIT® porque les ayuda a entender sus Sistemas de Información (o tecnologías de la información) y decidir el nivel de seguridad y control que es necesario para proteger los activos de sus compañías mediante el desarrollo de un modelo de administración de las tecnologías de la información.[2]

5.1.1.2 **Audiencia.**

Administración, Usuarios y Auditores. COBIT® está diseñado para ser utilizado por tres audiencias distintas:

- Administración/ gerencia (Management) Para ayudarlos a lograr un balance entre los riesgos y las inversiones en control en un ambiente de tecnología de información frecuentemente impredecible.

[2] *http://www.noguerakrb.net/index.php/component/content/article/25-the-project/46-cobitr*

- Usuarios: Para obtener una garantía en cuanto a la seguridad y controles de los servicios de tecnología de información proporcionados internamente o por terceras partes.
- Auditores: Para soportar su opinión y/o proporcionar consejos a la Administración sobre los controles internos[3].

5.1.1.3 **Beneficios de Implementar COBIT®.**

- Mejor alineación, con base en su enfoque de negocios
- Una visión, entendible para la gerencia, de lo que hace TI.
- Propiedad y responsabilidades claras, con base en su orientación a procesos.
- Aceptación general de terceros y reguladores
- Entendimiento compartido entre todos los participantes, con base en un lenguaje común.

5.1.1.4 **Criterios de Información de COBIT®.**

Para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos en COBIT® como requerimientos de información del negocio. Con base en los requerimientos de calidad, fiduciarios y de seguridad, se definieron los siguientes siete criterios de información:

[3] *Directrices Gerenciales Julio de 2000 3ra Edición. Publicado por El Comité de Dirección de COBIT® y el IT Governance InstituteTM*

- La efectividad tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable.
- La eficiencia consiste en que la información sea generada optimizando los recursos (más productivo y económico).
- La confidencialidad se refiere a la protección de información sensitiva contra revelación no autorizada.
- La integridad está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.
- La disponibilidad se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne con la protección de los recursos y las capacidades necesarias asociadas.
- El cumplimiento tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas.
- La confiabilidad significa proporcionar la información apropiada para que la gerencia administre la entidad y ejercite sus responsabilidades fiduciarias y de gobierno.

5.1.1.5 **Procesos Orientados COBIT®**.

Define las actividades de TI en un modelo genérico de procesos en cuatro dominios. Estos dominios son Planear y Organizar, Adquirir e Implementar,

Entregar y Dar Soporte y Monitorear y Evaluar. Los dominios se equiparan a las áreas tradicionales de TI de planear, construir, ejecutar y monitorear.

El marco de trabajo de COBIT® proporciona un modelo de procesos de referencia y un lenguaje común para que cada uno en la empresa visualice y administre las actividades de TI. La incorporación de un modelo operacional y un lenguaje común para todas las partes de un negocio involucradas en TI es uno de los pasos iniciales más importantes hacia un buen gobierno. Para gobernar efectivamente TI, es importante determinar las actividades y los riesgos que requieren ser administrados. Éstos se pueden resumir como sigue:

- **Planear y Organizar (PO)** Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI pueda contribuir de la mejor manera al logro de los objetivos del negocio. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, se debe implementar una estructura organizacional y una estructura tecnológica apropiada.

- **Adquirir e Implementar (AI)** Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como la implementación e integración en los procesos del negocio. Además, el cambio y el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio.

- **Entregar y Dar Soporte (DS)** Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operacionales.

- **Monitorear y Evaluar (ME)** Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del

desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno.

5.1.1.6 **COBIT® Basado en Controles.**

Los procesos requieren controles. Control se define como las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una seguridad razonable que los objetivos de negocio se alcanzarán, y los eventos no deseados serán prevenidos o detectados y corregidos.

Un objetivo de control de TI es una declaración del resultado o fin que se desea lograr al implantar procedimientos de control en una actividad de TI en particular. Los objetivos de control de COBIT® son los requerimientos mínimos para un control efectivo de cada proceso de TI.

La gerencia operacional usa los procesos para organizar y administrar las actividades de TI en curso. COBIT® brinda un modelo genérico de procesos que representa todos los procesos que normalmente se encuentran en las funciones de TI, proporcionando un modelo de referencia general y entendible para la gerencia operacional de TI y para la gerencia administrativa. Para lograr un gobierno efectivo, los gerentes operacionales deben implementar los controles necesarios dentro de un marco de control definido para todos los procesos TI. Ya que los objetivos de control de TI de COBIT® están organizados por procesos de TI, el marco de trabajo brinda vínculos claros entre los requerimientos de gobierno de TI, los procesos de TI y los controles de TI.

Cada uno de los procesos de TI de COBIT® tiene un objetivo de control de alto nivel y un número de objetivos de control detallados. Como un todo, representan las características de un proceso bien administrado. Los objetivos de control detallados se identifican por dos caracteres que representan el dominio más un número de proceso y un número de objetivo de control.

Además de los objetivos de control detallados, cada proceso COBIT® tiene requerimientos de control genéricos que se identifican con PCn, que significa número de control de proceso. Se deben tomar como un todo junto con los objetivos de control del proceso para tener una visión completa de los requerimientos de control.

5.1.1.7 **Generadores de Mediciones**.

Una necesidad básica de toda empresa es entender el estado de sus propios sistemas de TI y decidir qué nivel de administración y control debe proporcionar la empresa.

La obtención de una visión objetiva del nivel de desempeño propio de una empresa no es sencilla. ¿Qué se debe medir y cómo? Las empresas deben medir dónde se encuentran y dónde se requieren mejoras, e implementar un juego de herramientas gerenciales para monitorear esta mejora.

Para decidir cuál es el nivel correcto, la gerencia debe preguntarse a sí misma: ¿Qué tan lejos debemos ir, y está justificado el costo por el beneficio?
COBIT® atiende estos temas por medio de:

- **Modelos de Madurez**. El modelado de la madurez para la administración y el control de los procesos de TI se basa en un método de evaluación de la organización, de tal forma que se pueda evaluar a sí misma desde un nivel de no-existente (0) hasta un nivel de optimizado (5). Este enfoque se deriva del modelo de madurez que el Software Engineering Institute definió para la madurez de la capacidad del desarrollo de software. Cualquiera que sea el modelo, las escalas no deben ser demasiado granulares, ya que eso haría que el sistema fuera difícil de usar y sugeriría una precisión que no es justificable debido a que en general, el fin es identificar dónde se encuentran los problemas y cómo fijar prioridades para las mejoras. El propósito no es avaluar el nivel de adherencia a los objetivos de control.

Los niveles de madurez están diseñados como perfiles de procesos de TI que una empresa reconocería como descripciones de estados posibles actuales y futuros. No están diseñados para ser usados como un modelo limitante, donde no se puede pasar al siguiente nivel superior sin haber cumplido todas las condiciones del nivel inferior. Si se usan los procesos de madurez desarrollados para cada uno de los 34 procesos TI de COBIT®, la administración podrá identificar:

- El desempeño real de la empresa —Dónde se encuentra la empresa
- El objetivo de mejora de la empresa —Dónde desea estar la empresa

Se ha definido un modelo de madurez para cada uno de los 34 procesos de TI, con una escala de medición creciente a partir de 0, no existente, hasta 5, optimizado.

- **0 No existente**. Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.
- **1 Inicial.** Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques ad hoc que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.
- **2 Repetible**. Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.
- **3 Definido**. Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.
- **4 Administrado.** Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y

proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.

- **5 Optimizado**. Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

La ventaja de un modelo de madurez es que es relativamente fácil para la dirección ubicarse a sí misma en la escala y evaluar qué se debe hacer si se requiere desarrollar una mejora. La escala incluye al 0 ya que es muy posible que no existan procesos en lo absoluto. La escala del 0-5 se basa en una escala de madurez simple que muestra como un proceso evoluciona desde una capacidad no existente hasta una capacidad optimizada.

En resumen, los modelos de madurez brindan un perfil genérico de las etapas a través de las cuales evolucionan las empresas para la administración y el control de los procesos de TI, estos son:

- Un conjunto de requerimientos y los aspectos que los hacen posibles en los distintos niveles de madurez.
- Una escala donde la diferencia se puede medir de forma sencilla. Una escala que se presta a sí misma para una comparación práctica. La base para establecer el estado actual y el estado deseado.
- Soporte para un análisis de brechas para determinar qué se requiere hacer para alcanzar el nivel seleccionado.
- Metas y mediciones de desempeño para los procesos de TI, que demuestran cómo los procesos satisfacen las necesidades del negocio y de TI, y cómo se usan para medir el desempeño de los procesos internos basados en los principios de un marcador de puntuación balanceado (balanced scorecard)
- Metas de actividades para facilitar el desempeño efectivo de los procesos.[4]

[4] *IT Governance Institute COBIT® 4.0*

5.1.2 **ISO 27001**

Esta norma ha sido elaborada para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI). La adopción de un SGSI debería ser una decisión estratégica para una organización.

El diseño e implementación del SGSI de una organización están influenciados por las necesidades y objetivos, los requisitos de seguridad, los procesos empleados y el tamaño y estructura de la organización. Se espera que estos aspectos y sus sistemas de apoyo cambien con el tiempo. Se espera que la implementación de un SGSI se ajuste de acuerdo con las necesidades de la organización, por ejemplo, una situación simple requiere una solución de SGSI simple.

Se puede usar para evaluar la conformidad, por las partes interesadas, tanto internas como externas. Además promueve la adopción de un enfoque basado en procesos, para establecer, implementar, operar, hacer seguimiento, mantener y mejorar el SGSI de una organización.

Para funcionar eficazmente, una organización debe identificar y gestionar muchas actividades. Se puede considerar como un proceso cualquier actividad que use recursos y cuya gestión permita la transformación de entradas en salidas. Con frecuencia, el resultado de un proceso constituye directamente la entrada del proceso siguiente.

La aplicación de un sistema de procesos dentro de una organización, junto con la identificación e interacciones entre estos procesos, y su gestión, se puede denominar como un "enfoque basado en procesos".

El enfoque basado en procesos para la gestión de la seguridad de la información, presentado en esta norma, estimula a sus usuarios a hacer énfasis en la importancia de:

- Comprender los requisitos de seguridad de la información del negocio, y la necesidad de establecer la política y objetivos en relación con la seguridad de la información.
- Implementar y operar controles para manejar los riesgos de seguridad de la información de una organización en el contexto de los riesgos globales del negocio de la organización.
- El seguimiento y revisión del desempeño, eficacia del SGSI, y la mejora continua basada en la medición de objetivos.

Esta norma adopta el modelo de procesos "Planificar-Hacer-Verificar-Actuar" (PHVA), que se aplica para estructurar todos los procesos del SGSI. La adopción del modelo PHVA también reflejará los principios establecidos en las Directrices OCDE (2002)[5] que controlan la seguridad de sistemas y redes de información. Esta norma brinda un modelo robusto para implementar los principios en aquellas directrices que controlan la evaluación de riesgos, diseño e implementación de la seguridad, gestión y reevaluación de la seguridad.

5.1.2.1 **Compatibilidad con otros Sistemas de Gestión**.

Está alineada con la NTC-ISO 9001:2000 y la NTC-ISO 14001:2004, con el fin de apoyar la implementación y operación, consistentes e integradas con sistemas de gestión relacionados. Un sistema de gestión diseñado adecuadamente puede entonces satisfacer los requisitos de todas estas normas.

Esta norma está diseñada para permitir que una organización alinee o integre su SGSI con los requisitos de los sistemas de gestión relacionados[6].

---

[5] *Directrices OCDE para la seguridad de sistemas y redes de información. Hacia una cultura de la seguridad. París: OCDE, Julio de 2002. www.oecd.org.*
[6] *Estandar Internacional ISO 27001 Primera edición 2005-10-15*

5.1.3 **ISO 27005**

Publicada el 4 de Junio de 2008. Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. El conocimiento de los conceptos, modelos, procesos y términos descritos en la norma ISO/IEC 27001 e ISO/IEC 27002 es importante para un completo entendimiento de la norma ISO/IEC 27005:2008, que es aplicable a todo tipo de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro) que tienen la intención de gestionar los riesgos que puedan comprometer la organización de la seguridad de la información. Su publicación revisa y retira las normas ISO/IEC TR 13335-3:1998 y ISO/IEC TR 13335-4:2000.[7]

La norma ISO/IEC 27005:2008 sustituye (y actualiza) las partes 3 y 4 de la norma ISO TR 13335 (Técnicas para la gestión de la seguridad IT y Selección de salvaguardas, respectivamente) y se convierte en la guía principal para el desarrollo de las actividades de análisis y tratamiento de riesgos en el contexto de un SGSI. Constituye, por tanto, una ampliación del apartado 4.2.1 de la norma ISO 27001, en el que se presenta la gestión de riesgos como la piedra angular de un SGSI, pero sin prever una metodología específica para ello.

A su vez, se recomienda conocer las normas ISO/IEC 27001e ISO/IEC 27002 para entender el funcionamiento de la ISO/IEC 27005:2008[8]

5.1.4 **ITIL**

A finales de los 80 nació ITIL (Information Technology Infrastructure Library), que se ha convertido en un estándar de facto mundial para la Gestión del Servicio de

[7] *http://www.iso27000.es/download/doc_iso27000_all.pdf*
[8] *https://www.inteco.es/wikiAction/Seguridad/Observatorio/area_juridica_seguridad/Enciclopedia/Articulos_1/iso_27005_en*

las Tecnologías de la Información, proveyendo un conjunto cohesionado de mejores prácticas que abarcan tanto el sector público como el privado.

ITIL es la metodología más reconocida a nivel mundial para la definición de todos los procesos relacionados con la administración de IT. Pertenece al OGC (Office of Government Commerce), previamente conocido como CCTA (Central Computer and Telecommunications Agency), un departamento del gobierno del Reino Unido, y fue desarrollado durante fines de los 80.

La versión 2, ITIL describe todos los procesos necesarios para organizar la Gestión del Servicio de las TI con vistas a garantizar los niveles de servicio acordados entre la organización de TI y sus clientes. Estos procesos están focalizados en las mejores prácticas que pueden ser utilizadas de formas distintas para adaptarse a las diferentes necesidades.

La versión 3 (mayo 2007) revisa profundamente la versión anterior dirigiendo en esta ocasión su mirada a los servicios ofrecidos y su "ciclo de vida", siendo su principal objetivo la alineación con las líneas estratégicas de la organización. Da un especial énfasis a activo que supone las TI para la organización.

5.1.4.1 **Beneficios de ITIL**.

- Una mejora de la calidad de los servicios proveídos.
- Una visión clara y más confianza de los servicios ofrecidos de TI.
- Una visión clara de la capacidad actual de TI.
- Mayor flexibilidad para las organizaciones a través de un entendimiento con las TI.
- Un personal más satisfecho, a través de un mayor entendimiento de la capacidad y mejores expectativas de gestión.
- Mayor flexibilidad y adaptabilidad.

- Mejora en los sistemas, tales como seguridad, fiabilidad, velocidad y disponibilidad como se requiere en el nivel de servicio a ofrecer.
- Reducción del tiempo de los cambios que se efectúan y una tasa mayor de éxito.
- Alineación de los servicios de TI con las necesidades de las organizaciones definidas.
- Asegura una mejor comunicación entre TI y las organizaciones a través de un lenguaje común
- Mejora la calidad y reduce los costes a largo plazo de la provisión de los servicios.
- Crea una base sólida para la mejora continua.
- Incrementa la transparencia y control de las organizaciones de TI.

ITIL a su vez permite:

- Mejor accesibilidad a los servicios por parte de los usuarios a través de un punto de contacto definido.
- Más rapidez en las respuestas a las peticiones y quejas de los clientes.
- Mejora del trabajo en equipo y la comunicación.
- Mejor identificación de las áreas de mejora.
- Una visión proactiva (solucionar problemas).
- Reducir impactos negativos sobre las actividades de las organizaciones.
- Un uso más eficaz y eficiente de los recursos de TI.
- Reducción de las paradas debidas a los sistemas de TI.
- Mejora en los ratios de resolución de incidencias.
- Mejor control de los acuerdos a nivel de servicio.

- Descubrimiento e implementación de soluciones permanentes.
- Una aproximación consistente y sistemática a todos los procesos.

ITIL es una de las herramientas que permite, mediante su conjunto de buenas prácticas orientadas al negocio, a procesos y a clientes/usuarios conseguir una óptima Gestión del Servicio y los beneficios que ello implica.[9]

5.1.5 **MYSQL**

MySQL es un sistema gestor de bases de datos que se puede encuadrar dentro de la categoría de los programas open-source (es aquel cuyo código fuente está disponible para los usuarios y abierto a modificaciones)

5.1.5.1 **Orígenes e Historia de MySQL**.

MySQL es un caso particular, pues se trata de un programa de licencia open-source y gratuito pero que, sin embargo, está mantenido por una empresa, MySQL AB, con sede en Suecia.

El código fuente de MySQL está sólo relativamente abierto y disponible para modificaciones, puesto que es la empresa MySQL AB la que contrata y coordina los trabajos de mantenimiento del producto. No obstante, los trabajadores contratados, procedentes de todo el mundo, son usuarios del producto que realizan sus encargos a través de Internet.

El origen de MySQL se remonta a la década de los ochenta. Michael Widenius, también conocido como Monty, un joven programador que realizaba complejas aplicaciones en lenguaje BASIC, al no encontrar un sistema de

[9] *algunas definiciones se tomaron de ITIL v2 Books, ITIL v3 Books, www.lucidit.com.au*

almacenamiento de archivos que le resultara satisfactorio, pensó en construir el suyo propio.

Años después, en 1995, y en colaboración con David Axmark, Widenius desarrolló un producto que básicamente era el resultado de sus investigaciones, más dos aportaciones nuevas: el uso del lenguaje SQL y la accesibilidad a través de Internet. Así nació MySQL y también la empresa MySQLAB.

5.1.5.2 **Evolución**.

La evolución de MySQL se produce con las sugerencias de los usuarios, canalizadas por la empresa MySQL AB, que contrata a programadores de todo el mundo para que, a través de Internet, vayan ampliando y mejorando el producto.

Las versiones, como es costumbre en este tipo de software libre, se van colgando en Internet para que los usuarios puedan disponer de ellas. Sin embargo, también como es habitual, hay que distinguir entre versiones de prueba o beta y versiones estables o de producción.

5.1.5.3 **Características de MySQL.**

Aparte de las características que definen MySQL como programa open-source, existen aspectos que lo diferencian de otros productos como, por citar uno conocido, Access. Los atributos a los que hacemos referencia son:

- Posibilidad de crear y configurar usuarios, asignando a cada uno de ellos permisos diferentes.

- Facilidad de exportación e importación de datos, incluso de la base de datos completa.
- Posibilidad de ejecutar conjuntos de instrucciones guardadas en ficheros externos a la base de datos.[10]

5.1.6 **PHP**

Se trata indudablemente del lenguaje script de servidor más popular. Fue el primero en aparecer aunque realmente empezó a imponerse en torno al año 2000 por encima de ASP que era la tecnología de servidor reinante. Hoy en día se puede instalar módulos para interpretar PHP en casi todos los servidores de aplicaciones web. En especial PHP tiene una gran relación con Apache.

Es un lenguaje basado en C y en Perl, que se ha diseñado pensando en darle la máxima versatilidad y facilidad de aprendizaje, por encima de la rigidez y coherencia semántica.

5.1.6.1 **Ventajas de PHP.**

- **Multiplataforma.** A diferencia de otros lenguajes (especialmente de ASP y ColdFussion), se puede lanzar en casi todas las plataformas de trabajo (Windows, Linux, Mac,…)
- **Abierto y gratuito.** Pertenece al software licenciado como GNU, la licencia del sistema Linux; lo que permite su distribución gratuita y que la comunidad mejore el código.
- **Gran comunidad de usuarios.** La popularidad de PHP, junto con la gran defensa que de él hacen los defensores del código abierto, permite tener una comunidad amplia y dinámica a la que acudir en caso de necesidad.

[10] *Base de datos y software libre. Mysql básico 08 - http://www.sinemed.com/recursos/docs/MySQL.pdf*

- **Apache, MySQL.** Apache es el servidor web y de aplicaciones más utilizado en la actualidad. MySQL es el servidor de bases de datos relacionales más popular en Internet para crear aplicaciones web. Puesto que PHP tiene una gran relación y compatibilidad con ambos productos, esto se convierte en una enorme ventaja.
- **Extensiones.** Dispone de un enorme número de extensiones que amplía las capacidades del lenguaje, facilitando la creación de aplicaciones web complejas.

5.2 MARCO CONCEPTUAL

Activo: Es un bien que se utiliza para la operación de la entidad.

Acuerdos de Servicio: Los acuerdos de servicios pueden ser internos y externos y básicamente es la reglamentación o contrato estipulado entre las partes involucradas en un proceso para su cumplimiento, estos poseen la operación o servicio de responsabilidad de cada una de las partes en horarios, penalizaciones, responsabilidades etc. Existen los SLA (Service Level Agreement) acuerdos de nivel de servicio y los OLA (Operational Level Agreements) acuerdos de nivel operacional.

Ambiente de Desarrollo: Corresponde al espacio físico y virtual dispuesto para creación de aplicaciones, aquí son desarrolladas y probadas a nivel básico de funcionamiento realizadas por los desarrolladores.

Amenazas: Son los eventos que pueden desencadenar un incidente, produciendo daños materiales o inmateriales en los activos.

Antivirus: Programa cuya finalidad es prevenir los virus informáticos así como curar los ya existentes en un sistema.

Aplicación: Cualquier programa que corra en un sistema operativo y que haga una función específica para la automatización de una actividad o proceso en el negocio, como por ejemplo aplicaciones de monitoreo, registro y control sobre las necesidades de un negocio.

Base de Datos: Conjunto de datos que pertenecen al mismo contexto almacenados sistemáticamente. En una base de datos la información se organiza en campos y registros. Los datos pueden aparecer en forma de texto, números, gráficos, sonido o vídeo.

Cables de Red: Son aquellos alambres que permiten conectar a las computadoras entre sí o a terminales de redes y es por medio de estos que los bits se trasladan.

Centro de Cómputo: Corazón operacional de una compañía que tenga como base fundamental de los procesos core del negocio el procesamiento de información. Generalmente se encuentran dentro de las instalaciones de la compañía y almacenan gran cantidad de servidores y equipos de comunicaciones, poseen condiciones de seguridad físicas y ambientales adecuadas para la conservación de los equipos: entre las condiciones mínimas que debe tener un centro de cómputo esta los siguientes: control de acceso optimo, conexiones al interior y exterior de la compañía con gran velocidad, sensores de humo, extintores, pisos y techos falsos, señalización, herramientas de monitoreo de alertas, temperaturas no superiores a los 17 grados, adecuada ubicación(bajo nivel de riesgo).

Consultoría: Es un servicio de ayuda a las organizaciones para mejorar su funcionamiento, principalmente analizando la existencia de problemas comerciales y desarrollando planes para mejorar. Una consultoría se lleva a cabo por empresas o personas, llamadas consultores o consultoras, que son profesionales o empresas propiamente tales, especialistas en las materias que una organización necesita mejorar o que considera problemas a solucionar.

Contraseña: Password. Código utilizado para accesar un sistema restringido. Pueden contener caracteres alfanuméricos e incluso algunos otros símbolos. Se destaca que la contraseña no es visible en la pantalla al momento de ser tecleada con el propósito de que sólo pueda ser conocida por el usuario propietario de la cuenta.

Data Center: Lugar de almacenamiento de servidores y equipos de comunicación; tiene todas las facilidades de ancho de banda, seguridad física, aire acondicionado, cámaras de seguridad, etc. Se usa principalmente para empresas que quieran almacenar equipos de contingencia en lugares externos a su sitio de operación con el fin de sobrevivir ante catástrofes naturales, incendio, asonadas etc.

Dominio: Sistema de denominación de hosts en Internet el cual está formado por un conjunto de caracteres el cual identifica un sitio de la red accesible por un usuario. Los dominios van separados por un punto y jerárquicamente están organizados de derecha a izquierda. Comprenden una red de computadoras que comparten una característica común, como el estar en el mismo país, en la misma organización o en el mismo departamento. Los más comunes son .com, .edu, .net, .org, .biz, .info.

Firewall: Combinación de hardware y software. Un firewall es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su acceso, un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

Hosting: El alojamiento web (en inglés web hosting) es el servicio que provee a los usuarios de Internet, un sistema para poder almacenar información, imágenes, vídeo, o cualquier contenido accesible vía Web. El alojamiento web o alojamiento de páginas web, se refiere al lugar que ocupa una página web, sitio web, sistema, correo electrónico, archivos etc. en Internet o más específicamente en un servidor que por lo general hospeda varias aplicaciones o páginas web.

Impacto: Efecto del riesgo sobre la organización.

Infraestructura Tecnológica: Está compuesta por Hardware, Software, bases de datos, telecomunicaciones, personas y procedimientos todos configurados para recolectar, manipular, almacenar y procesar datos para ser convertidos en información.

Manuales de Usuario: corresponde a la descripción de uso o modo de empleo de una aplicación.

Política de Seguridad: Es el conjunto de normas y procedimientos establecidos por una organización para regular el uso de la información y de los sistemas que la tratan con el fin de mitigar el riesgo de pérdida, deterioro o acceso no autorizado a la misma.

Probabilidad: Es la frecuencia con la cual se podría materializar un riesgo.

Rack: Es un soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones. Las medidas para la anchura están normalizadas para que sean

compatibles con equipamiento de cualquier fabricante. También son llamados bastidores, cabinas, cabinets o armarios.

Riesgo: Se considera riesgo la estimación del grado de exposición de un activo, a que una amenaza se materialice sobre el causando daños a la organización. El riesgo indica lo que le podría pasar a los activos si no se protegen adecuadamente.

Servidor: Es una computadora que maneja peticiones de datos, email, servicios de redes y transferencia de archivos de otras computadoras (clientes). También puede referirse a un software específico.

Set de Pruebas: Corresponde al documento donde se describe el detalle de las pruebas a ejecutar en una aplicación antes de su paso al ambiente de producción, adicionalmente se documenta el resultado de la prueba y los ajustes a tener en cuenta según el resultado.

Sistema de Información: Conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de una empresa o negocio.

Sistema Operativo: Operating System (OS) en inglés. Programa especial el cual se carga en una computadora al prenderla, y cuya función es gestionar los demás programas, o aplicaciones, que se ejecutarán, como por ejemplo, un procesador de palabras o una hoja de cálculo, un juego o una conexión a Internet. Windows, Linux, Unix, MacOS son todos sistemas operativos.

Software: Se refiere a programas en general, aplicaciones, juegos, sistemas operativos, utilitarios, antivirus, etc. Lo que se pueda ejecutar en la computadora.

Sql: (Structured Query Language) es un lenguaje de consuta estructurado, surgido de un proyecto de investigación de IBM para el acceso a base de datos relacionales. Actualmente se ha convertido en un estándar de lenguaje de base de datos, la mayoría de los sistemas de base de datos lo soportan, desde sistems para ordenadores personales, hata grandes ordenadores.

Switch: Traducido significa interruptor. Se trata de un dispositivo inteligente utilizado en redes de área local (LAN - Local Area Network), una red local es aquella que cuenta con una interconexión de computadoras relativamente cercanas por medio de cables. La función primordial del Switch es unir varias redes entre sí, sin examinar la

información lo que le permite trabajar de manera muy veloz, ya que solo evalúa la dirección de destino, aunque actualmente se combinan con la tecnología Router para actuar como filtros y evitar el paso de tramas de datos dañadas.

TI: Se refiere al campo entero de la tecnología informática - que incluye hardware de computadoras y programación hasta administración de redes. La mayoría de las empresas medianas y grandes tienen departamentos de TI.

Topología de Estrella: La topología estrella es una de las topologías más populares de un LAN (Local Area Network). Es implementada conectando cada computadora a un Hub central. El Hub puede ser Activo, Pasivo o Inteligente. Un hub activo es solo un punto de conexión y no requiere energía eléctrica. Un Hub activo (el más común) es actualmente un repetidor con múltiples puertos; impulsa la señal antes de pasarla a la siguiente computadora. Un Hub Inteligente es un hub activo pero con capacidad de diagnóstico, puede detectar errores y corregirlos.

Ups: (Uninterruptible Power Supply). Es una fuente de suministro eléctrico que posee una batería con el fin de continuar suministrando energía a un dispositivo en el caso de interrupción eléctrica).

Usuario: Persona que utiliza o trabaja sobre una aplicación específica basado en permisos estipulados según su rol en una compañía.

Vulnerabilidad: es todo aquello que provoca que nuestros sistemas informáticos funcionen de manera diferente para lo que estaban pensados, afectando a la seguridad de los mismos, pudiendo llegar a provocar entre otras cosas la pérdida y robo de información sensible.

5.3 MARCO LEGAL

Conglomerado Técnico Colombiano S.A. – CONTECSA S.A, es una sociedad de naturaleza anónima. Dado que es una empresa legalmente constituida en Colombia, está regulada por las normas descritas en el **Código de Comercio** (Decreto 410 de 1971) y **Código Civil** (Ley 57 de 1887).

El objeto social de esta sociedad es adelantar en nombre propio o de terceros, cualquier actividad relacionada con la Consultoría y/o Construcción necesarias para llevar a cabo cualquier obra de ingeniería o arquitectura. Incluye –pero no se limita- a las áreas de ingeniería civil, eléctrica, hidráulica, sanitaria, montaje, economía, finanzas, informática, ambiental, gestión, administración, planeación, desarrollo, información explotación y/o comercialización de recursos naturales, control de calidad o de cualquier tipo de servicio o actividad conexa. La sociedad puede realizar inversiones permitidas por Ley, en el territorio Colombiano y en el exterior, así como también representar empresas extranjeras o multinacionales que pretendan realizar inversiones y/o actividades en Colombia o fuera del país.

5.4 MARCO ORGANIZACIONAL

La Empresa

http://www.contecsa-sa.com/

Figura 1. Logo CONTECSA S.A

La sociedad **Conglomerado Técnico Colombiano S.A. – CONTECSA S.A.**- fue constituida en Junio de 1997. Es una empresa dedicada a la ejecución de consultoría y/o construcción de obra civil. Actualmente, tienen a su cargo el proyecto de ampliación de la Doble Calzada Vía al Mar Ruta 90A. Se encuentran ubicados en la vía antigua a Puerto Colombia.

Misión

Somos una empresa de proyectos de ingeniería enfocada en la construcción de obras civiles de infraestructura que presta sus servicios a clientes privados y estatales garantizando la calidad de sus obras en un entorno seguro, saludable y en armonía con el medio ambiente, bajo el cumplimiento de los requisitos aplicables.

Satisfacemos a nuestros clientes, incentivamos el desarrollo de nuestro personal, cumplimos los compromisos con nuestros proveedores y mejoramos continuamente nuestros procesos, en búsqueda de lograr la permanencia y crecimiento en el mercado,

la generación de beneficios económicos para los accionistas, el bienestar para nuestros colaboradores y la comunidad, y el progreso del país.

Visión

Aumentar el posicionamiento en el país, siendo reconocidos como una de las principales empresas de construcción y líderes en obras de infraestructura vial, que da cumplimiento oportuno a los requisitos contractuales y brinda soluciones integrales a sus clientes.

Objetivos

CONTECSA S.A., además de realizar consultorías y ejecutar todo tipo de obras de ingeniería, se ha especializado en la construcción de vías y carreteras; el desarrollo de la empresa se ha caracterizado por la consecución de un objetivo primordial, "Garantizar una óptima calidad con un máximo de seguridad en todas nuestras obras", sin esta premisa difícilmente se explicaría la permanencia en este sector tan selectivo durante más de 10 años que acreditan nuestra experiencia.

El actual mercado de la construcción de vías y carreteras y el creciente nivel de exigencia de nuestros clientes, llevan a desarrollar en todos nuestros procesos productivos, modernizando y actualizando todos los factores que inciden en los mismos.

Gestión de Calidad

La Gerencia de CONTECSA S.A. consciente del compromiso en cumplir con los requisitos que contrae con sus clientes, pone a disposición todos los recursos necesarios para garantizar que los productos, servicios y actividades llevadas a cabo cumplan estrictamente sus especificaciones.

Para ello, CONTECSA S.A. ha establecido en su organización un Sistema de Gestión de Calidad, que apunta a mejorar la eficiencia de sus procesos continuamente, basados en

las normas y especificaciones establecidas que permitan certificar cada uno de sus proyectos.

Compromisos

Asegurar que las actividades y los proyectos desarrollados a nuestros clientes sean seguros, confiables y que cumplan con las especificaciones, normas, códigos aplicables y requisitos legales, como parte integral del programa de gestión de calidad brindando soporte a cada una de nuestras actividades, como se señala a continuación:

- Establecemos sistemas orientados a la prevención y no solo a la detección.
- Disminuimos el margen de riesgos y el manejo de errores, con la aplicación de programas de control de pérdidas.
- Desarrollamos programas para el mejoramiento de nuestros procesos, en los aspectos tecnológicos, medio ambiente y calidad.
- Comprometemos y motivamos a nuestro talento humano con el objetivo de buscar su participación en la gestión y desarrollo del Sistema De gestión De Calidad implementado.

En CONTECSA S.A. estamos comprometidos con la salud y seguridad de nuestro talento humano, dedicando todos los recursos que sean necesarios para garantizar cada una de nuestras actividades, evitando riesgos innecesarios sobre el trabajador, implementando los siguientes parámetros:

- Establecer y mantener al día procedimientos que permitan asegurar el cumplimiento de las leyes y reglamentos preventivos aplicables a cada uno de nuestros proyectos, mediante la implementación del programa de salud ocupacional.

- Establecer sistemas encaminados a la prevención de riesgos laborales, así como del medio ambiente.
- Documentar actualizar y comunicar la política preventiva a nuestro personal con el propósito de comprometerlos y motivarlos en la búsqueda de su participación en la gestión y desarrollo del sistema de prevención de riesgos laborales.
- Adecuar la política preventiva cuando, por modificación o incorporación de nuestras actividades, productos o servicios, cambien la naturaleza y magnitud de los riesgos laborales y adecuarla a las nuevas características.

Organigrama

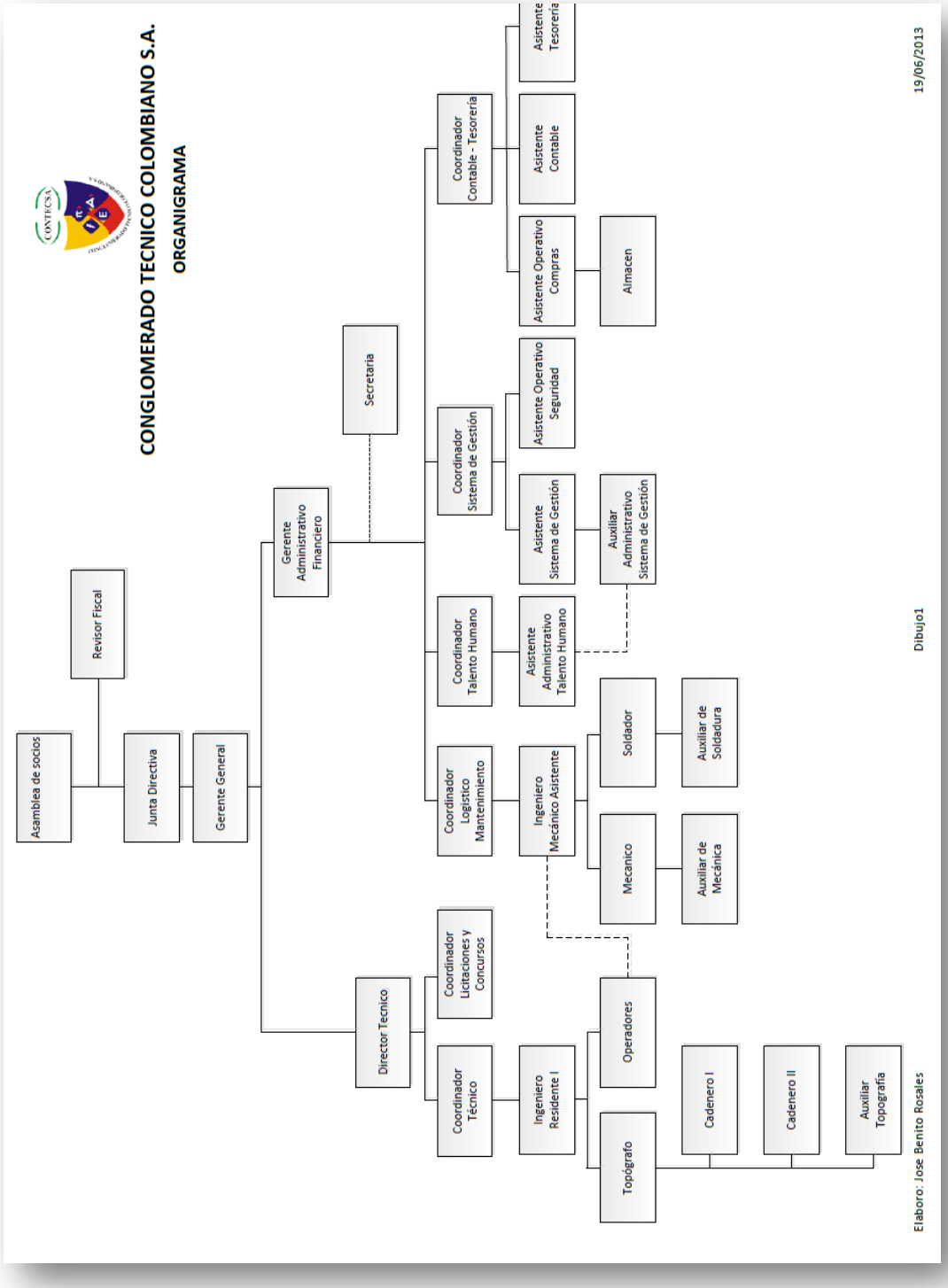


Figura 2. Organigrama CONTECSA S.A

6. DISEÑO METODOLÓGICO

6.1 ÁREA FOCO DE LA INVESTIGACIÓN

6.1.1 HARDWARE Y RED

Los temas relacionados con TI son administrados por el Sr. José Benito Rosales Martínez. CONTECSA tiene una infraestructura de red con tipología estrella, distribuido en tres (3) sedes de oficinas (administrativa e ingenierías). Los puntos de red convergen en la sede principal en un área condicionada de 3Mts^2, allí se encuentra ubicado un servidor Linux, donde está la instalada base de datos del programa SICON y tiene un disco duro espejo para reducir el riesgo por perdida de información, una UPS de 20kva, un rack 1.70 Mts., 1 switch 24 puertos. El cableado utilizado es Categoría 6e[11] que conectan a 22 equipos de escritorios (estaciones de trabajo) con similares características (ver anexo C). Existe un grupo de trabajo denominado CONTECSA, a través del cual, se comparten archivos y servicios de impresión. Cuentan con un acceso a Internet a través de Microonda con capacidad de 4MB.

6.1.2 SISTEMA OPERATIVO Y APLICACIONES

El ambiente de trabajo a nivel de usuario final es **Microsoft Windows®**, los programas ofimáticos que utilizan son **Microsoft Office®** y **Acrobat Profesional®**. El área financiera administra los temas contables con el aplicativo **World Office ver 7.0.12**. La gestión operativa utiliza principalmente el aplicativo SICON, que es una aplicación desarrollada por la organización a través de un tercero[12], y también aplicaciones de diseño como **Autocad®** y de presupuestos **Construdata®**. El servicio de Hosting es provisto por la firma **Bluehost**, por lo tanto, delegan a éste las actividades de seguridad y respaldo.

[11] *Alcanza frecuencias de 250Mhz y velocidades en cada par hasta 1Gbps*
[12] *Ingeniero de Sistemas - Desarrollador*

6.1.3 SISTEMA DE INFORMACIÓN CONTECSA – SICON

SICON (ver anexo A y B) es una aplicación en ambiente web, que tiene como objetivo agilizar las tareas propias de la gestión operativa en CONTECSA, es decir, la información relevante para el área técnica como por ejemplo: el cálculo de cargas de arena de los camiones, la información técnica u hoja de vida de los equipos utilizados en obra, información del personal que labora, compras y almacenamiento, informes. Todas estas actividades se realizaban de forma manual, es por eso que se tomó la decisión de iniciar un proyecto, con la finalidad de crear un software a su medida y así, agilizar el acceso y el proceso de la información. Se contrató a un Ingeniero desarrollador quien realizó el levantamiento de las necesidades y desarrolló para CONTECSA esta aplicación, que hoy día sigue actualizándose por módulos, hasta llegar a una meta próxima que es que la información que se genere en el trabajo de campo sea ingresada al sistema a través de dispositivos inalámbricos, actualizando al instante la base de datos, el cual es considerado como el óptimo desempeño de esta gestión a través de esta aplicación. Está aplicación está desarrollada en PHP versión 5, y utiliza Mysql para su gestión de base de datos.

6.1.4 NECESIDADES DE LAS PARTES

La alta gerencia de CONTECSA mostró un marcado interés con relación a la puesta en marcha de este proyecto, porque es consciente de la importancia de las tecnologías de la información para lograr sus metas y obtener una ventaja competitiva en el mercado de firmas constructoras especializadas en el sector de vías y movimiento de tierras.

En principio, está interesada en obtener un diagnóstico profesional y objetivo de cómo se realizan las actividades TI. Adicionalmente, le interesa una guía que le permita mejorar sus procesos de TI. La información y las recomendaciones consignadas en los informes producto de ésta Consultoría, les ofrecerán una alternativa de mejoramiento bajo un concepto claro, que sin duda, serán un aporte significativo al plan de mejoramiento de la calidad que se implementa en

CONTECSA S.A., y su desarrollo descriptivo se podrá configurar como un apoyo eficaz para una gestión administrativa y de control y orientado a la utilización óptima de sus recursos de TI.

Para los autores, el desarrollo de la Consultoría brinda la oportunidad de adquirir experiencia al emplear los conocimientos y las técnicas adquiridos durante la participación en la Especialización en Auditoría a los Sistemas de Información y optar por el título académico.

6.1.5 FORMALIZACIÓN DE LA ACTIVIDAD

La Gerente General, Dra. Diana Rodríguez Isidro, impartió su aprobación mediante un comunicado (ver Anexo D). Luego de esto, se diligenció un Acuerdo de Confidencialidad entre las partes (ver anexo E) en el que se pactaron acuerdos de no divulgación de información, firmados por CONTECSA y los consultores.

6.1.6 MÉTODO DE ESTUDIO

Para el desarrollo de esta Consultoría, se utilizó primordialmente un enfoque de **investigación de campo** (presencial en el ámbito de la empresa, para recolección de información tanto primaria como secundaria y para observación directa de procesos con fines analíticos y de auditoría). La mirada que se imprime sobre los resultados recogidos en la fase de **campo** se basa en un **modelo descriptivo de análisis**, para el cual se parte de los **marcos conceptuales y modelos en uso de la Auditoria Informática y la Administración del Riesgo**. De manera especial, el enfoque de la metodología aplicada se orienta hacia un mejoramiento de las actividades de la gestión informática de la empresa.

La metodología y técnicas de auditoría informática implementadas se inspiran en la necesidad de disponer de la identificación del entorno, el desarrollo, la aplicabilidad y el uso de la infraestructura TI aplicado en CONTECSA, es decir, software, hardware, componentes pasivos y activos de red. Asimismo, tiene lugar el planteamiento de los controles pertinentes para garantizar un ambiente de seguridad.

6.1.7 RESTRICCIÓN METODOLÓGICA

Mientras se ejecutaba esta Consultoría, se difundió la versión 5.0 (ver anexo H) del COBIT®. Sin embargo, para efectos del desarrollo de esta Consultoría y propósitos académicos se acordó utilizar COBIT® 4.1, de tal manera que una vez se hayan implementado las recomendaciones pertinentes, pueda escalarse hacía la versión 5.0.

6.1.8 DISEÑO DE LA INVESTIGACIÓN

Esta Consultoría por ser considerada un proyecto factible contempló la elaboración y desarrollo de técnicas de auditoria viables como las entrevistas y la aplicación de pruebas de validación, cuyo propósito principal fue la generación de recomendaciones, previa identificación del entorno, las fortalezas y debilidades del proceso materia de esta consultoría.

6.1.9 TIPO DE INVESTIGACIÓN

Dada su desarrollo esta investigación se puede clasificar en la modalidad de tipo campo, documental y descriptiva, debido a que las técnicas aplicadas permitieron la recolección de información directa, que consintió un análisis objetivo en base a datos y documentación recolectada.

6.1.10 POBLACIÓN Y MUESTRA

En el desarrollo de toda investigación es fundamental determinar el espacio donde se desarrolla y los individuos generadores y/o procesadores de información. La muestra representa una parte de la población objeto de estudio.

La muestra total se delimitó al personal Técnico-Administrativo (5 Personas) que tienen el contacto directo tanto con la infraestructura TI, el aplicativo SICON, y la toma de decisiones, todos ellos ubicados en la sede de CONTECSA S.A. A continuación los describimos:

	Nombre	Cargo	Área
1	Diana Patricia Rodríguez Isidro	Gerente General	Administrativa
2	Gerardo Antonio Hernández Salazar	Gerente Administrativo y Financiero	Administrativa
3	José Benito Rosales Martínez	Director Técnico	Administrativo
4	Freddy Leonardo González Vergara	Coordinador Contable y Financiero	Contabilidad
5	Heberto Andrés Martínez Quintero	Ingeniero Auxiliar	Técnica
6	Luis Barraza Jimeno	Ingeniero Desarrollador	Contratista Tercerizado

Tabla 1. Funcionarios Entrevistados

6.1.11 TÉCNICAS Y HERRAMIENTAS DE RECOLECCIÓN DE INFORMACIÓN

En principio, se hizo un reconocimiento preliminar de la empresa, a través de la solicitud de documentación pertinente y relevante como son su manual de calidad, mapas de procesos, organigrama, las políticas de seguridad de la información. Esto permitió obtener una definición objetiva y la ubicación del proceso objeto de esta consultoría.

La realización de visitas físicas, permitió la comprobación de los puestos de trabajo de los usuarios finales y el desarrollo de pruebas técnicas al azar. Se utilizó la entrevista como técnica principal para obtención de información y el instrumento fueron los cuestionarios que contenían preguntas cerradas y abiertas como opciones, las cuales una vez procesadas dieron a los consultores argumentos para el desarrollo de los respectivos informes.

6.1.12 PROCEDIMIENTO PARA EL ANÁLISIS DE LOS RESULTADOS

Una etapa inicial denominada, etapa descriptiva, en donde los datos se observaron, comprobaron y recolectaron, luego, se dio paso la etapa interpretativa donde se glosaron y juzgaron los datos obtenidos. La tercera etapa fue la prospectiva en donde se asumió una posición frente al volumen de información lo que permitió evaluarla. Estas etapas permitieron analizar la información lo que condujo a la identificación y el análisis y las deducciones pertinentes en función de los objetivos propuestos en este proyecto.

6.1.13 INFORMACIÓN DE LOS RESPONSABLES DE LA CONSULTORÍA

Todos los ejecutores de esta consultoría son profesionales aspirantes al título de Especialistas en Auditoria a los sistemas de Información, titulo otorgado por la Universidad de la Costa.

	Nombre	Detalle
1	Ana María Molinares Donado	Ingeniera de Sistemas, Universidad Autónoma de Colombia (2.001) T.P. 08255126377ATL
2	Lenys Rangel Ferrer	Ingeniera de Sistemas, Universidad Simón Bolivar (2.007) T.P. 0825523324ATL
3	Manuela Maria Villar Ávila	Ingeniera de Sistemas, Universidad del Norte (2.010) T.P.08255217296ATL

Tabla 2. Consultores

7. INFORMES DE LA CONSULTORÍA

7.1 INFORME EJECUTIVO

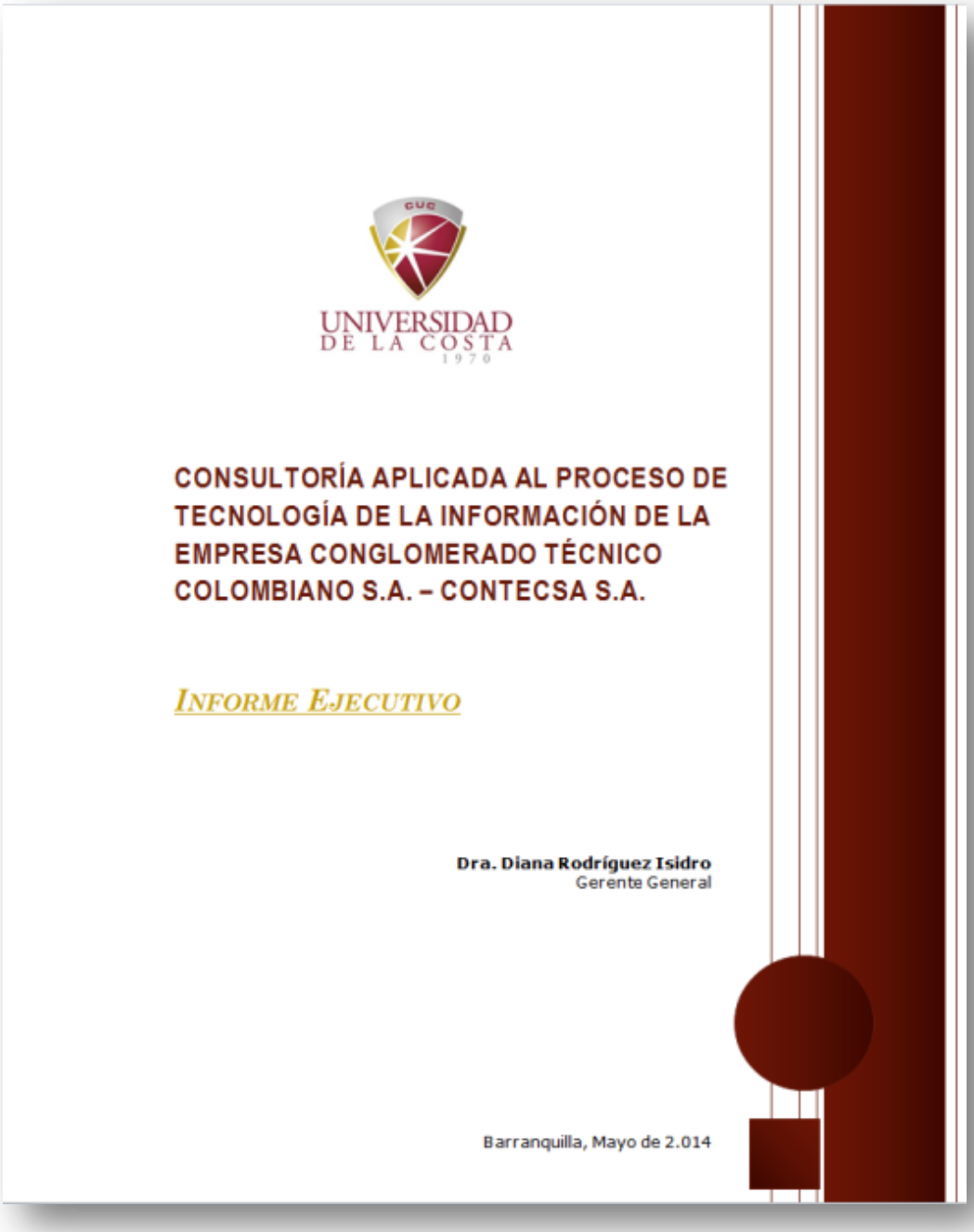


Figura 3. Portada Informe Ejecutivo

Barranquilla, Mayo 7 de 2.014

Doctora
DIANA PATRICIA RODRIGUEZ ISIDRO
Gerente General
E. S. M.

Ref.: Informe Ejecutivo de la Consultoría aplicada al Proceso de Tecnología de la Información en CONTECSA.

Cordial Saludo.

Adjunto a este comunicado, hacemos entrega oficial del informe en referencia, para su revisión y análisis.

De antemano, muchas gracias por la oportunidad y el soporte brindados. En espera de sus comentarios,

Cordialmente,

Ana Molinares **Lenys Rangel** **Manuela Villar**

7.1.1 INTRODUCCIÓN

El desarrollo de esta Consultoría centró su hacer en realizar un estudio sobre el cómo CONTECSA S.A gestiona los temas relacionados con la tecnología informática, es decir, desde su estructura implementada hasta los procesos de adquisición, administración y desarrollo teniendo como referencia el estándar COBIT®[13] 4.1. Todo lo anterior, con la finalidad de proporcionar a CONTECSA una serie de recomendaciones tendientes a coadyuvar su compromiso para el mejoramiento de sus procesos.

7.1.2 METODOLOGÍA EMPLEADA

Se evaluaron las estrategias y políticas relacionadas con la administración, planeación, organización y control del proceso de TI relacionadas con el desarrollo y mantenimiento de los sistemas informáticos en CONTECSA mediante entrevistas, solicitud de documentación relevante, asimismo, se realizó un reconocimiento directo de su infraestructura y sobre los proyectos a corto, mediano y largo plazo en los temas relacionados a TI.

Las recomendaciones a lugar se plantean siguiendo una serie de estándares internacionalmente acerca de la seguridad de la información reconocidos como Mejores Prácticas. Cabe anotar que mientras se ejecutaba esta Consultoría, se difundió la versión 5.0 (ver anexo G) del COBIT®. Sin embargo, para efectos del desarrollo de esta Consultoría se acordó entre las partes, utilizar COBIT® 4.1, de tal manera que una vez se hayan implementado las recomendaciones pertinentes, pueda escalarse hacía la versión 5.0.

El análisis de riesgos asociados al proceso de TI en CONTECSA, le permitirá tomar decisiones más acertadas que apuntarán a que este proceso este alineado a la visión de la empresa.

---

[13] COBIT® es un marco de referencia desarrollado para la administración de procesos de TI con un fuerte enfoque en el control

7.1.3 DESCRIPCIÓN DE LA CONSULTORÍA

En general se realizaron las siguientes actividades:

- ✓ Revisión de la **gestión o ciclo de vida TI** en CONTECSA.
  - Se solicitó documentación y/o procedimientos operativos para evaluar el diseño conceptual la estructura en general y sobre el programa SICON.
  - Se ejecutaron **pruebas de aceptación**[14] **y de sistema**[15] sobre el programa SICON.
  - Se comparó el **entorno TI** con los controles propuestos por los estándares bases propuestos por esta Consultoría.

- ✓ Revisión de los **mecanismos de control** de acceso a los servicios informáticos.
  - Se revisaron los mecanismos de **control de acceso lógico** del usuario a los recursos de la red.
  - Se revisó el acceso lógico de los usuarios para limitar el acceso a la información desde la aplicación SICON.
  - Se revisó la correcta implementación de **los controles de filtrado de tráfico** en los firewall.
  - Se hizo revisión de la **seguridad perimetral**.
  - Se verificó que se exista un **análisis de vulnerabilidades**.

- ✓ Realización de **Entrevistas**
  - Se entrevistó al funcionario encargado de coordinar las tareas de TI
  - Se entrevistaron a los usuarios finales del programa SICON
  - Se conversó con algunos funcionarios técnicos-administrativos a medida que se inspeccionan los equipos.

---

[14] *Pruebas aplicadas sobre el producto terminado e integrado, concebidas para que sea un usuario final quien detecte los posibles errores.*
[15] *Prueba aplicada al producto terminado y su objetivo es ver la respuesta del sistema en su conjunto simulando varias alternativas*

7.1.4 LIMITACIONES DE LA CONSULTORÍA

Documental. En general, no se evidenció documentación relacionada con la planeación de proyectos de TI, Diseños de la aplicación SICON, manuales de usuario, políticas de seguridad.

7.1.5 CONCLUSIONES PRINCIPALES

7.1.5.1 Fortalezas.

- ✓ Se percibe un ambiente de deseo por mejorar la gestión de los procesos de TI.
    - La actitud de la alta gerencia demuestra pleno interés en aplicar las recomendaciones pertinentes producto de esta investigación.
    - El personal administrativo tiene un elevado grado de compromiso y sentido de pertenencia con la organización y su futuro.
- ✓ El proyecto de generar una aplicación que automatizara el proceso misional contribuyó a la reducción del tiempo para la generación de informes, sus planes de cobertura a través de internet garantizaron tener acceso a la información al instante.
- ✓ El mantenimiento preventivo (limpieza de hardware) a los equipos de usuario final es efectivo y documentado.
- ✓ Existe un inventario de activos de TI actualizado.
- ✓ La empresa utiliza el ambiente web para acceder a sus servicios informáticos y darse a conocer ante sus posibles clientes.

7.1.5.2 **Debilidades.**

- ✓ Ausencia de un área o departamento de TI específico en el organigrama de la empresa destinada a la administración como tal de los proyectos de TI. Estos son tratados como un proyecto adicional y no queda claro su categoría como proceso de apoyo para la organización.

- ✓ No se ha vinculado un profesional con el perfil adecuado para la administración de los procesos de TI.

- ✓ Planeación estratégica mínima, se realiza como se necesite en respuesta a un requerimiento de negocio específico.

- ✓ Carencia de Políticas de Seguridad de la información

- ✓ Ausencia y por tanto, no disponibilidad de un diseño detallado del programa SICON y sus actualizaciones, así como el desarrollo y la puesta en marcha del mismo, no fue modelado por una estructura de proyecto sólida, que minimizara los riesgos para la aplicación de este tipo de proyectos.

- ✓ Ausencia y por tanto, no disponibilidad de documentación relacionada con las modificaciones y actualizaciones sobre el programa SICON.
- ✓ Carencia de un control de cuentas de usuario final.

- ✓ El control de tráfico de información la red local es nulo

- ✓ La administración básica en la red local no ha sido definida.

- ✓ No existe un control sobre las instalaciones de software, ni los suplementos de seguridad críticos.

- ✓ No están debidamente identificados, ni valorados los riesgos de TI.

7.1.5.3 **Hallazgos**.

- ✓ Carencia de políticas de seguridad que normalicen el hacer de los usuarios de los servicios informáticos ofrecidos en la empresa, y que a su vez, permitan establecer conciencia a través de un ambiente de control.

- ✓ No se practica una evaluación cabal en materia de asignación de los privilegios o permisos administrativos a usuarios finales sobre el sistema operativo.

- ✓ La documentación de las actividades que se ejecutan en general es mínima y en algunos casos, inexistente, lo que dificulta una adecuada trazabilidad en respuesta a un evento o a un requerimiento de información.

- ✓ La adquisición de recursos de TI es casuística. Vale decir no se dispone de una política definida para tal fin. No es suficiente apoyarse en el precio de un producto o la oportunidad de una oferta, se requiere de un análisis objetivo y enfoques estructurados que conlleven a una decisión adecuada y al cumplimiento del propósito deseado.

- ✓ La confidencialidad, la disponibilidad e integridad de la información están expuestas a un perfil de vulnerabilidades y riesgos con una gran probabilidad de ocurrencia.

- ✓ Aunque las capacitaciones para el uso del aplicativo SICON han demostrado ser efectivas, es necesario establecer procedimientos estructurados –que hoy no existen- para este fin, con el objeto de minimizar los errores de uso del aplicativo.

- ✓ Aunque el servidor donde se encuentra la base de datos SICON tiene un disco duro espejo, no existe una política de respaldo que disminuya la posibilidad de pérdida de información ante un evento no deseado.

- ✓ El proceso de administración de cambios en el programa SICON es informal. Las autorizaciones se realizan de manera verbal. Los compromisos y alcances

de las partes no se documentan. Adicionalmente, en el evento de la inefectividad de un cambio –esto es, que éste no arroje los resultados esperados- se hace necesario estar advertidos de la ponderación de los correspondientes productos colaterales no deseados, ni deseables, así como de los impactos o efectos negativos que se presenten. De igual manera, se precisa acotar e identificar las responsabilidades de los actores.

7.1.5.4 **Riesgos.**

- ✓ Acceso no autorizado a la red Interna
- ✓ Ataques Informáticos
- ✓ Bajo nivel de utilización de las TI como ventaja competitiva
- ✓ Base y/o Guías de Conocimientos Focalizadas.
- ✓ Pérdida de la Información.
- ✓ Desempeño Operacional Inadecuado de la Infraestructura de TI.
- ✓ Falta de Disponibilidad, Confidencialidad e Integridad de la Información.
- ✓ Fraude Electrónico.
- ✓ Inadecuada Gestión de Proveedores de TI.
- ✓ Inadecuado cumplimiento del Gobierno de TI.
- ✓ Incumplimiento Regulatorio Legales.
- ✓ Incumplimiento de acuerdos en proyectos de TI.
- ✓ Indeterminabilidad de Acciones y Responsabilidades (No Trazabilidad).
- ✓ Insatisfacción del Cliente Interno de los Servicios de TI.
- ✓ Lineamientos de TI no acordes con la estrategia del negocio.
- ✓ Medición no confiable y por ende, Irrelevancia del Indicador Coso-Beneficio de la Tecnología.

7.1.5.5 **Modelo de Madurez de COBIT®**.

El modelo de madurez para la administración y el control de los procesos de TI se basan en un método de evaluación para la organización, de tal forma que se pueda valorar desde una caracterización en escala de 0 a 5. …Véase el numeral 7.2.10 en el informe detallado…

COBIT® ayuda a las empresas a establecer un valor óptimo desde las TI, equilibrando el beneficio y la optimización entre los niveles de riesgo y el uso de los recursos, además, los principios que el COBIT aplica son genéricos y útiles para las organizaciones de cualquier tamaño, bien sean comerciales, sin ánimo de lucro o públicas.

A través de este método de medición, se puede interpretar qué tan bien están desarrollados los procesos de TI en CONTECSA hoy, es decir, qué tan capaces son en realidad y qué tan bien desarrollados o capaces deberían ser –esto depende principalmente de las necesidades del negocio establecidas.

En la siguiente imagen, establecemos de manera general el nivel actual de CONTECSA frente a las recomendaciones del deber ser que plantea COBIT®.

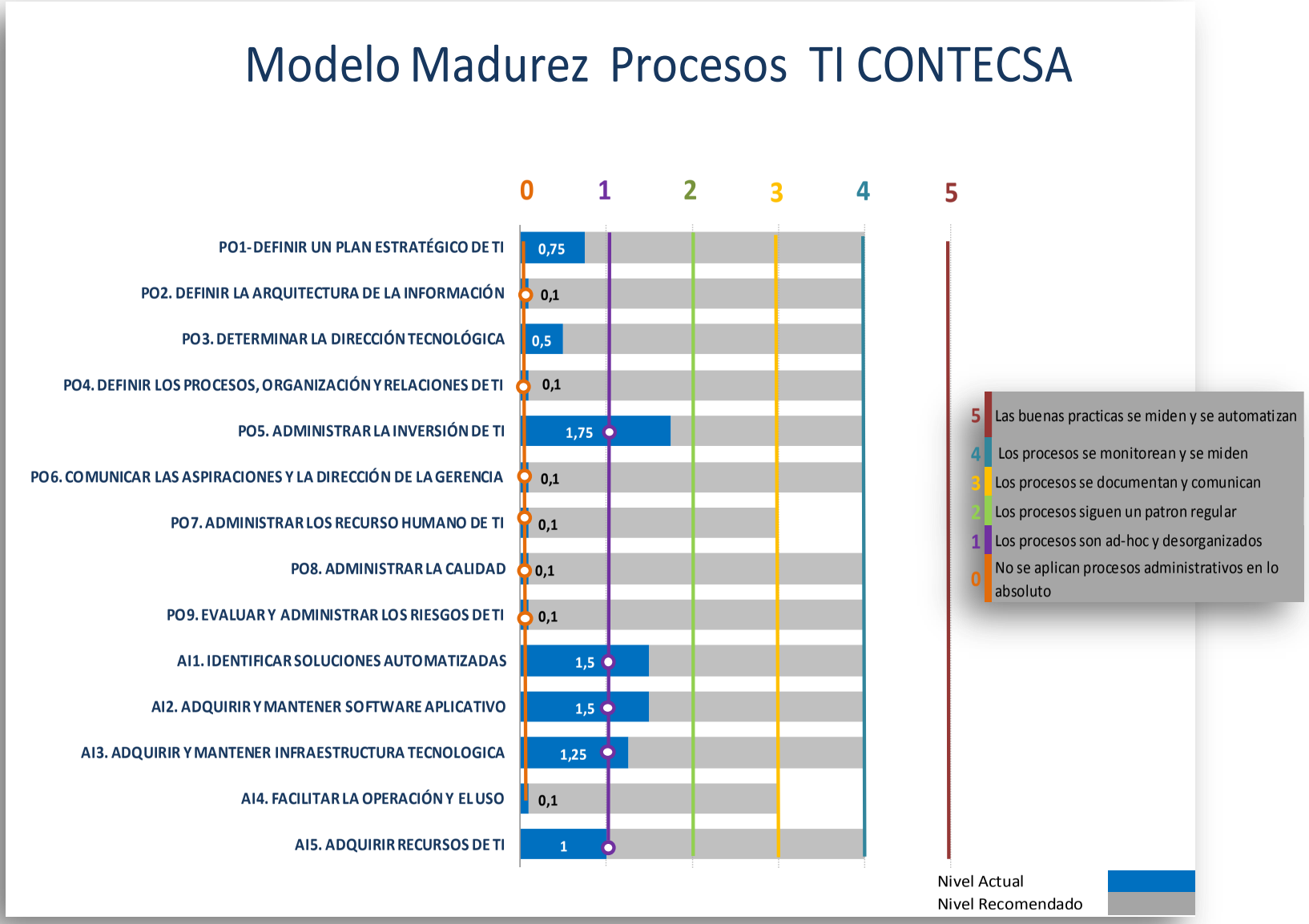


Figura 4. Modelo de Madurez COBIT ® aplicado a CONTECSA

7.1.5.6 **OPINIÓN DE LA CONSULTORÍA**

Los hallazgos obtenidos en esta Consultoría comparten una raíz causal común: **Una gestión de TI frágilmente estructurada. En términos generales, habida consideración de la importancia de las TI como proceso de apoyo para CONTECSA, esta condición se traduce en una administración de recursos y servicios vulnerable, riesgosa e inadecuada.**

7.1.5.7 **RECOMENDACIONES**

Sujetos a los lineamientos descritos por los marcos de referencia utilizados para la ejecución de esta Consultoría, se precisa un listado de recomendaciones que al establecerse, actuarán como controles que mitigarán el impacto en el evento de ocurrencia de uno de los riesgos descritos.

- ✓ Realizar un estudio sobre las necesidades de aplicaciones de los usuarios.
- ✓ Desarrollar y aplicar procedimientos de adquisición de TI que satisfagan los requerimientos del negocio.
- ✓ Adquirir legalmente las licencias correspondientes de inmediato.
- ✓ Implementar Políticas de manejo y uso sobre los recursos de TI
- ✓ Restringir los permisos de instalaciones sobre los equipos.
- ✓ La Gerencia debe asumir la responsabilidad de proporcionar recursos para la implementación y divulgación de un ambiente de control que promocione las buenas prácticas internas en la empresa.
- ✓ Definir e implementar políticas de seguridad de TI.

- ✓ La Gerencia debería asegurar que todo el personal al que se le asigne responsabilidades o que participa en TI sea competente para realizar las tareas asignadas.
- ✓ Es oportuno controlar el tráfico (entrante y saliente) de la información en la red.
- ✓ Concientización e intervención de la alta gerencia para la alineación de los objetivos de TI con los objetivos del negocio.
- ✓ Definir un Plan Estratégico para TI.
- ✓ Ubicar a TI dentro de la estructura organizacional. Definición de Roles y Funciones.
- ✓ Desarrollar prácticas adecuadas de supervisión dentro de la función de TI.
- ✓ Implementar una metodología para la identificación y evaluación de soluciones TI, cuyo objetivo equilibre las necesidades de la organización en tiempo y costo.
- ✓ Generar procedimientos para establecer, modificar y concluir contrato que apliquen a los proveedores.
- ✓ Implementar prácticas para la selección de proveedores.
- ✓ Realizar un contrato con el proveedor por el tiempo o los módulos que se encuentren pendientes.
- ✓ Desarrollar prácticas adecuadas de supervisión dentro de la función de TI.
- ✓ Instalar aplicaciones licenciadas que garanticen las actualizaciones liberadas por los proveedores.
- ✓ Implementar una adecuada segregación de funciones.
- ✓ Generar procedimientos de captura de conocimiento (Documentación).
- ✓ Implementar una política de respaldo adecuada.
- ✓ Fomentar la concientización de seguridad de la información.

7.2 INFORME DETALLADO

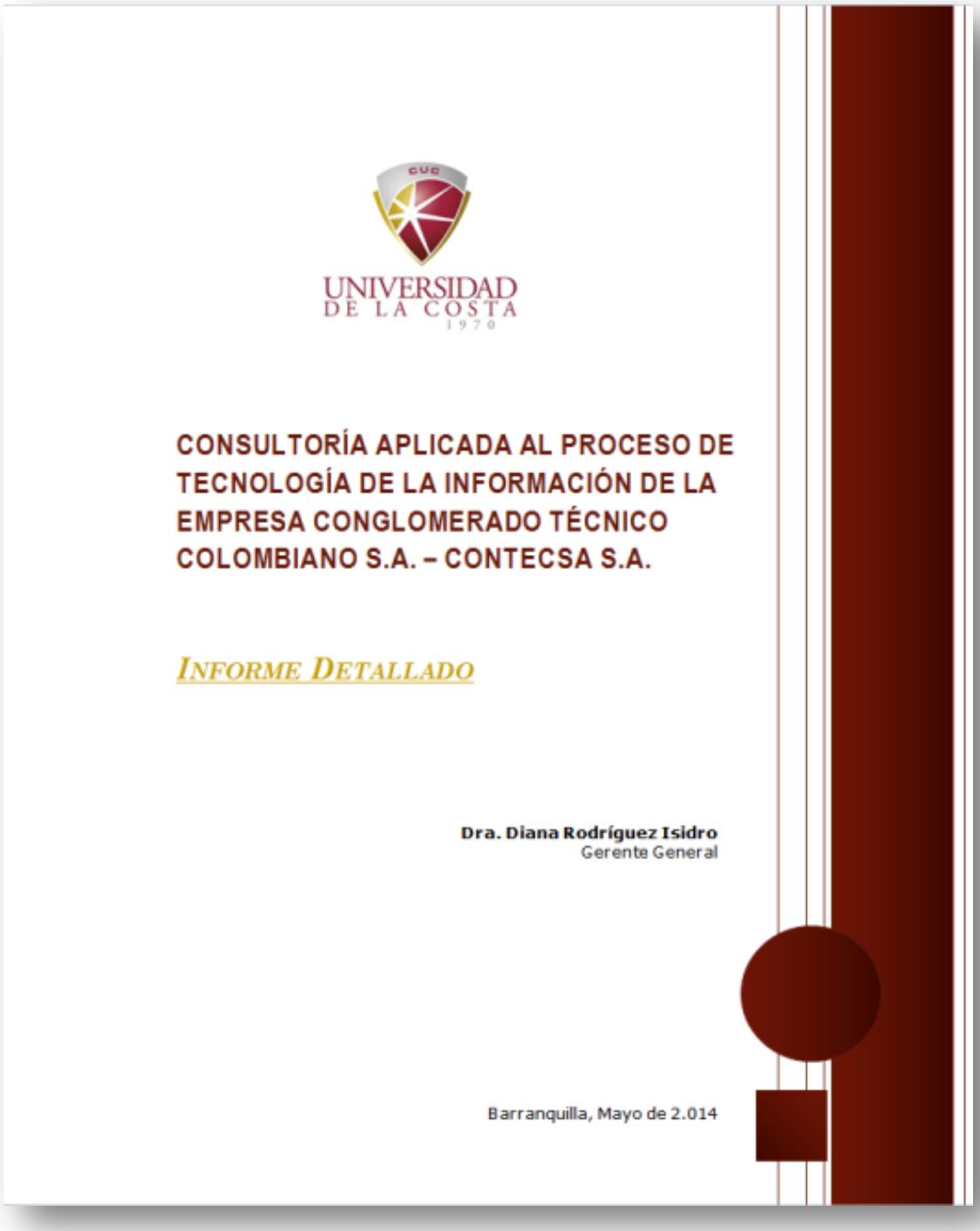


Figura 5. Portada Informe Detallado

Barranquilla, Mayo 7 de 2014

Doctora
DIANA PATRICIA RODRIGUEZ ISIDRO
Gerente General
E. S. M.

Ref.: **Informe Detallado** de la Consultoría aplicada al proceso de Tecnología de la Información en CONTECSA.

Cordial Saludo.

Adjunto a este comunicado, hacemos entrega oficial del informe en referencia, para su revisión y análisis.

De antemano muchas gracias por la oportunidad, en espera de sus comentarios.

Cordialmente,

Ana Molinares **Lenys Rangel** **Manuela Villar**

7.2.1 INTRODUCCIÓN

Este documento, ofrece una información más específica y detallada sobre las vulnerabilidades detectadas y recomendaciones producto de esta Consultoría, que a su vez, ayudará a CONTECSA en la toma de decisiones estratégicas que mejoren el desempeño de las TI en la organización, y en general, el desempeño de los demás procesos que se apoyan en éste, generando un impacto positivo sobre el desempeño global de la organización, sobre su imagen corporativa y especialmente, ante sus clientes.

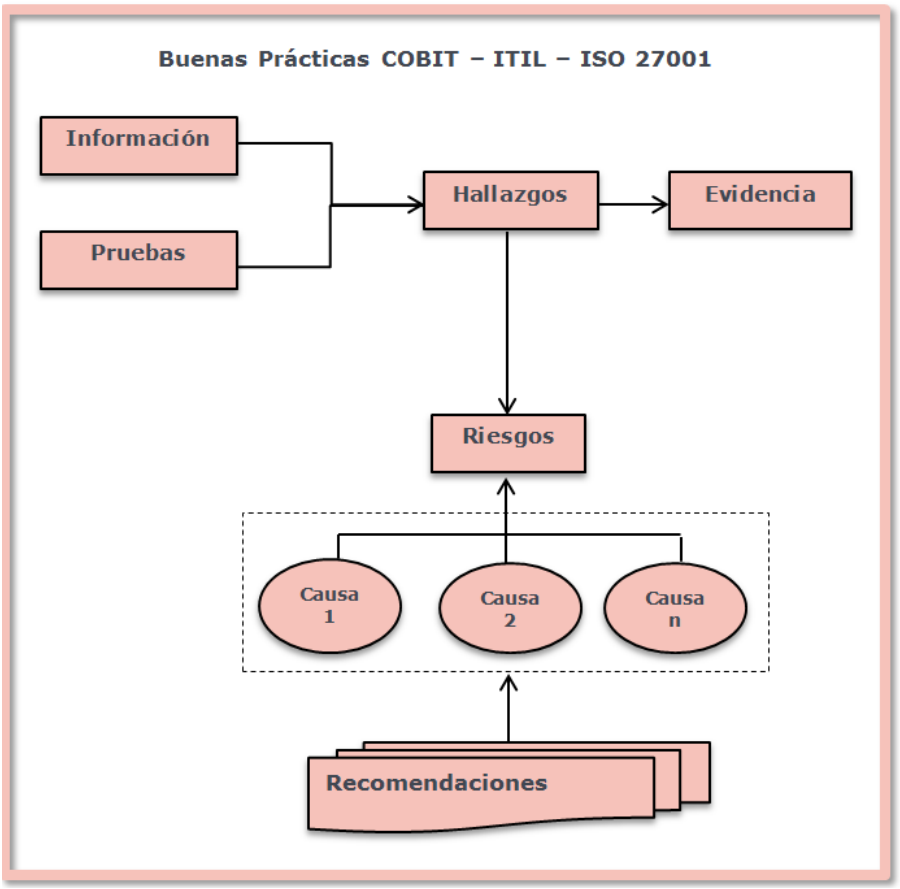


Figura 6. Estructura Lógica de la Consultoría

En la imagen anterior se graficó las herramientas, entradas, procesos y salidas de esta Consultoría, con el objeto de facilitar la interpretación de la misma, siguiendo una estructura lógica, es decir, se observa en la figura que las recomendaciones descritas en este informe, apuntan a las causas que generan los riesgos, a los cuales CONTECSA está potencialmente expuesta. Lo anterior, obedeciendo la guía enmarcada por las buenas prácticas en TI

Las actividades relacionadas para la ejecución de esta Consultoría obedecieron a la estructura descrita en el Programa de Consultoría siguiente:

7.2.2 **PROGRAMA DE CONSULTORÍA**

PROGRAMA DE CONSULTORÍA				N° 001 Duración: 6 meses
Empresa: Conglomerado Técnico Colombiano S.A. – CONTECSA				
Objetivo: Realizar una Consultoría a la empresa CONGLOMERADO TÉCNICO COLOMBIANO S.A. –CONTECSA S.A., específicamente a los sistemas de información e infraestructura tecnológica, basándonos en los estándares de buenas prácticas como COBIT ® 4.1, ISO 27001, ISO 27005 e ITIL® V3.				
Recursos: Humanos, Tecnológicos e Información.				
ETAPA	**ACTIVIDADES**	**RESPONSABLE**	**HORAS ESTIMADAS**	**FECHA**
Inicial	Visita a la página Web de la Organización para conocer el entorno.	Grupo Consultor	1H	11/07/2013
	Elaboración de la Propuesta de Consultoría.	Grupo Consultor	2H	11/07/2013
	Socialización de necesidades. Aceptación de la Propuesta.	CONTECSA	2H	12/07/2013
	Diligenciamiento del Acuerdo de Confidencialidad.	CONTECSA-Grupo Consultor	1H	12/07/2013
I. Planeación	Carta de Inicio de la Consultoría	Grupo Consultor	1H	14/07/2013

	Estudio del entorno y la estructura Organizacional, Procesos, Datos, Recursos y operaciones	Grupo Consultor	5H	09/11/2013
	Definición y desarrollo de un plan de trabajo, con el fin de definir el objetivo y el alcance de la consultoría.	Grupo Consultor	5H	12/11/2013 y 13/11/2013
	Elaboración de cuestionarios, entrevista, *checklist*.	Grupo Consultor	1H	14/11/2013
II. Ejecución	Entrevista a funcionarios que interactúan directamente con las TI de la empresa CONTECSA.	Grupo Consultor	7H	23/11/2013 y 30/11/2013
	Revisión General a las aplicaciones en uso, hardware, seguridad física, lógica e identificación de controles implementados.	Grupo Consultor	10H	11/01/2014 13/01/2014 y 18/01/2014
	Acceso con privilegios administrativos al aplicativo SICON, para revisión y ejecución de pruebas de validación y operatividad.	Grupo Consultor	9H	05/02/2014 08/02/2014 y 12/02/2014
	Obtención de evidencias.	Grupo Consultor	3H	13/02/2014
	Identificar y definir el nivel de madurez con base al estándar Cobit® 4.1	Grupo Consultor	12H	22/02/2014 26/02/2014 a 15/03/2014
	Análisis de información, discusión de los hallazgos, elaboración del mapa de riesgo.	Grupo Consultor	7H	22/03/2014 27/03/2014 y 29/03/2014
	Identificación de los riesgos latentes y materializados.	Grupo Consultor	6H	05/04/2014 y 12/04/2014
III. Revisión y Preinforme	Elaboración del borrador.	Grupo Consultor	5H	16/04/2014 y 19/04/2014
	Revisión de los papeles de trabajo	Grupo Consultor	4H	26/04/2014
	Elaboración de carta de presentación.	Grupo Consultor	3H	03/05/2014
IV. Informes	Elaboración.	Grupo Consultor	5H	04/05/2014 06/05/2014
	Presentación de los informes	CONTECSA-Grupo Consultor	1H	07/05/2014

7.2.3 LEVANTAMIENTO DE INFORMACIÓN

7.2.3.1 Reconocimiento de la Empresa y su Proceso TI.

Entrevistados:

- ✓ Diana Rodríguez – Gerente General
- ✓ Gerardo Hernández – Gerente Financiero

Objetivos:

- ✓ Reconocimiento de la Empresa.
- ✓ Revisión de las políticas, regulaciones, normas y procedimientos.
- ✓ Identificación del proceso de TI en la empresa.

	Cuestionario
1	¿Qué es CONTECSA?
2	Puede suministrarnos información relevante de la empresa como su misión, visión, organigrama, procesos, procedimientos…?
3	¿Cuántos empleados laboran en la empresa? Por favor clasifíquelos
4	¿Qué leyes regulan la actividad y/ gestión de CONTECSA?
5	¿Han tenido informes de auditoría anteriores? ¿Sobre qué área?
6	¿Existen procedimientos adecuados para mantener la documentación al día?
7	¿Existe algún mecanismo que permita a los empleados hacer sugerencias sobre mejoras en la organización del área?
8	¿Existe un documento donde este especificado la relación de las funciones y obligaciones del personal?
9	¿Existe un área encargada de las tecnologías de la información en la empresa?
10	¿Quién se encarga de la adquisición de tecnología?
11	¿Quién autoriza la compra de esta adquisición?
12	¿De dónde se obtienen los recursos y cómo se registran?
13	¿Cómo está compuesta la infraestructura tecnológica de la empresa?
14	¿Existen políticas de seguridad informática en la organización? De ser afirmativa la respuesta, necesitaríamos consultarlas.

15	¿Son estás políticas conocidas por los funcionarios?
16	¿A través de qué medio se divulgan estas políticas?
17	¿Qué tipos de Sistemas de Información tienen implementados?
18	¿Se ha realizado una planificación estratégica del o de los sistema(s) de información para la empresa?
19	¿Quiénes participan en esta planeación?
20	¿Existe una metodología para llevar a cabo tal planificación?
21	¿Los cambios en los sistemas informáticos son consecuencia de la planificación o presión por necesidades operativas?
22	¿Existe algún proyecto programado en el área de sistemas a corto, mediano o largo plazo?
23	Cómo se asignan las prioridades para las necesidades tecnológicas en la empresa?
24	¿Se lleva un control documentado sobre los cambios realizados a los equipos de la empresa?
25	¿Se capacita y concientiza a los empleados en seguridad de la información?
26	¿Existen y se tienen documentadas políticas para la contratación de servicios a terceros?
27	¿Se firman contratos de confidencialidad al momento de contratar con un tercero la prestación o adquisición de un servicio?
28	¿Tienen un inventario de los activos informáticos? De ser afirmativa la respuesta, necesitaríamos consultarlo.
29	Existe algún cronograma de mantenimiento preventivo? De ser afirmativa la respuesta, necesitaríamos consultarlo.
30	¿Se maneja un control sobre los activos informáticos por ejemplo hojas de vida?
31	¿Tienen servidores de datos?
32	¿Qué sistema operativo tiene de base?
33	¿Tienen servidores de seguridad?
34	¿Se disponen de directrices marcadas en algún plan informático?
35	¿Cómo se controla el avance de los proyectos en TI?
36	Los servicios de mantenimiento de la infraestructura informática (hardware y software) ¿Quién o cómo se realiza y cada cuanto se realizan?
37	¿Existe documentado un plan de seguridad de la información dentro de la organización?

38	¿Se maneja respaldo de la información?
39	¿Es este manual o automático?
40	¿Quién se encarga de realizarlos?
41	Describa la infraestructura de red implementada (rack, tipo de cableado, cantidad de puntos voz y datos, corriente regulada, supresores de voltaje, switches, router inalámbricos…)
42	¿Tienen conexión a internet?
43	¿Quiénes tienen acceso a internet?
44	¿Existen restricciones hacía los usuarios para acceder a internet o instalar programas?
45	¿Cuentan con una conexión a internet de respaldo?

7.2.3.2 **Evaluación Física.**

Entrevistados:

- ✓ José Benito Rosales – Director Técnico

Objetivos:

- ✓ Examinar de las políticas y Normas sobre seguridad Física.
- ✓ Verificar la seguridad de personal, datos, hardware, software e instalaciones

	Cuestionario
1	¿Existen medidas de seguridad sobre los activos informáticos y el centro de cómputo?
2	¿Existe una persona responsable de la Seguridad?
3	¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad?
4	¿Existe personal de vigilancia en la institución?
5	¿Existe una clara definición de funciones entre los puestos clave?
6	Se investiga a los vigilantes cuando son contratados directamente?
7	¿Se controla el trabajo fuera de horario?
8	¿Existen registros de las acciones de los usuarios?
9	¿Existe vigilancia en las oficinas y el centro de cómputo las 24 horas?

10	¿Se permite el acceso a los archivos y a las aplicaciones a todos los usuarios?
11	¿Se ha instruido al personal de seguridad sobre las medidas a tomar en caso de que alguien pretenda entrar sin autorización?
12	¿El centro de cómputo tiene salida al exterior?
13	¿Son controladas las visitas al centro de cómputo y a los puestos de trabajo?
14	¿Se registra el acceso al departamento de cómputo de personas ajenas a TI?
15	¿Se vigilan la moral y comportamiento del personal con el fin de mantener una buena imagen y evitar un posible fraude?
16	¿Se ha adiestrado el personal en el manejo de los extintores?
17	¿Se revisa de acuerdo con el proveedor el funcionamiento de los extintores?
18	¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?
19	¿Se ha instruido al personal que hacer en caso de una emergencia por fuego?
20	¿Se ha prohibido a los usuarios el consumo de alimentos y bebidas en los puestos de trabajo y el interior del centro de cómputo?
21	Se cuenta con respaldos de información en un lugar distinto al de la computadora?
22	¿Se tienen establecidos procedimientos de actualización a estas copias?
23	¿Existe departamento de auditoria interna en la institución?

7.2.3.3 **Evaluación de las Aplicaciones.**

Entrevistados:

- ✓ José Benito Rosales – Director Técnico
- ✓ Luis Barraza – Ingeniero Desarrollador
- ✓ Freddy González - Contador
- ✓ Heberto Martínez - Profesional

Objetivos:

- ✓ Identificar de la metodología aplicada.
- ✓ Verificar el control de cambios.
- ✓ Reconocer el software y las aplicaciones actualmente en uso.
- ✓ Revisar la seguridad, utilidad, confianza, privacidad y disponibilidad de la información.

	Cuestionario
1	¿Qué software se utiliza en Contecsa?
2	¿Poseen licencias para el uso de estas aplicaciones?
3	¿Considera que la aplicación cumple su objetivo?
4	¿Qué es SICON?
5	¿Cuál es el lenguaje de programación utilizado?
6	¿Cómo fue el proceso de selección y contratación para el desarrollo de este aplicativo?
7	¿Existe un contrato para esta actividad de desarrollo?
8	¿Existen proyectos a corto, mediano o largo plazo?
9	¿Cuáles?
10	¿Existe un cronograma de actividades?
11	¿Existe respaldo de la Información?
12	¿Existe documentación detallada sobre los cambios aplicados al programa?
13	¿Dónde es el lugar de desarrollo?
14	¿Cómo se realizan las pruebas?
15	¿Existen manuales del sistema?
16	¿Existen manuales de usuario Final?
17	¿Existen niveles de acceso en las aplicaciones?
18	¿Existen logs?

7.2.4 REVISIÓN DE LA DOCUMENTACIÓN

Se solicitaron y revisaron:

- ✓ Controles propuestos por la norma para ver si están implementados y si estos son idóneos.
- ✓ Cronograma de actividades para determinar el cumplimiento.
- ✓ Licenciamiento de Software.
- ✓ Soportes de Mantenimientos preventivos ejecutados.
- ✓ Contrato del Desarrollo de la aplicación SICON.
- ✓ Listado de roles y perfiles del aplicativo SICON
- ✓ Manuales de diseños y de usuario final para la aplicación SICON
- ✓ Procedimientos operativos de instalación.

7.2.5 EJECUCIÓN DE PRUEBAS TÉCNICAS

- ✓ Se buscan configuraciones e instalaciones de equipos y elementos de la infraestructura de TI.
- ✓ Se hace un análisis de vulnerabilidades en las configuraciones de los equipos.
- ✓ Se revisan la autenticación y validación de los usuarios en el aplicativo SICON.
- ✓ Se ejecutan los cálculos en el aplicativo SICON.

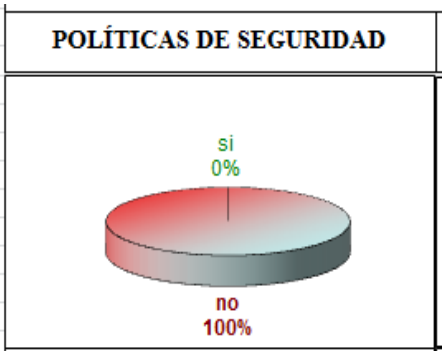
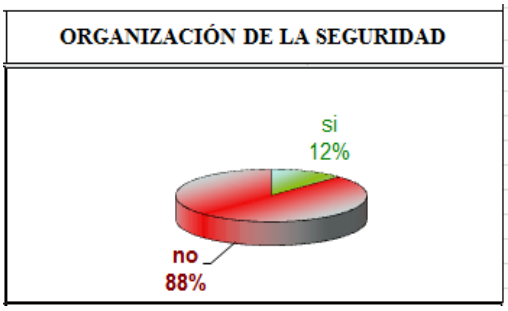
7.2.6 ANÁLISIS E INTERPRETACIÓN

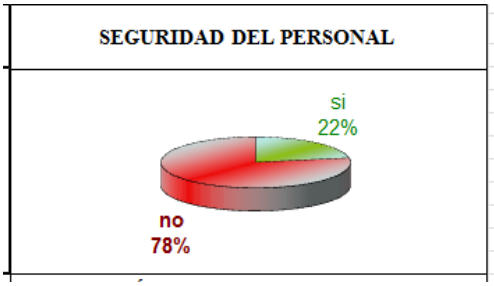
En este apartado del informe, se describe detalladamente los hallazgos, las pruebas ejecutadas y las recomendaciones pertinentes, resultados de la aplicación de las técnicas y las herramientas desarrolladas en la interpretación de los marcos de referencia propuestos para la aplicación de esta Consultoría.

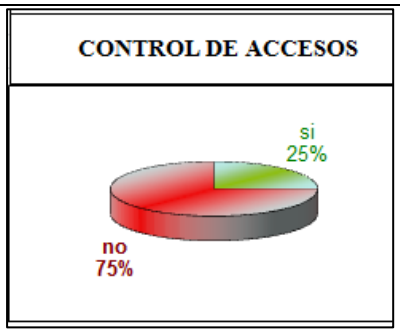
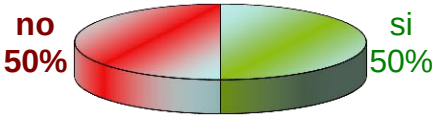
7.2.6.1 **Diagnóstico ISO 27001.**

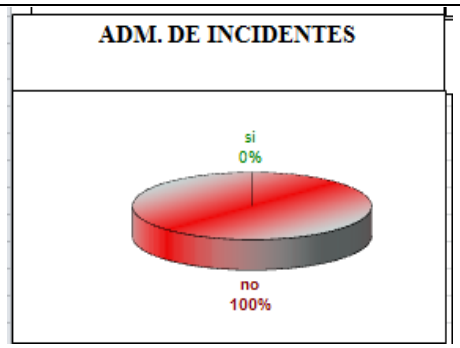
Teniendo como entrada la información recolectada a través de las diferentes entrevistas, se ejecutó este modelo de diagnóstico que la ISO 27001 tiene como base de referencia para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI). Consiste en un check list Verdadero (Sí) o Falso (No), al finalizarlo, obtenemos un análisis sobre la situación actual de TI en CONTECSA, representados gráficamente los porcentajes obtenidos. (Ver Anexo F).

- Graficas de Resultados Test ISO 27001

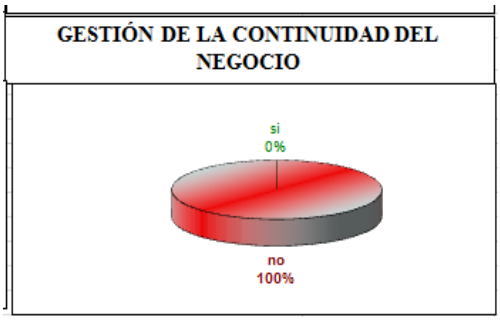
 Ausencia absoluta de políticas de seguridad definida y documentada.	 No se tiene el perfil adecuado, ni responsable en la seguridad de los sistemas de información. Por ende no existe ningún criterio de seguridad en el manejo de terceras partes.

 Se lleva control primario de los activos de hardware actualizados. Sin embargo, no existe control sobre el software utilizado.	 No existen medidas implementadas para la seguridad de la información que es manejada por el personal. Existe una formación básica para el tratamiento de los activos.

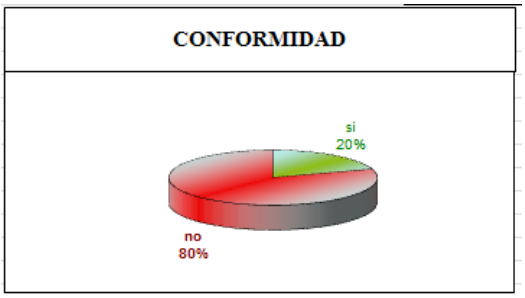
 Mínimo control de acceso. Sin embargo, existen restricciones de usuario a través de perfiles para acceder al aplicativo SICON en autenticación.	**DESARROLLO Y MANTENIMIENTO DE SISTEMAS**  Se tiene establecidos algunos requisitos en la etapa de implementación o desarrollo del software para que sea seguro. Aunque no cuenta con una estructura de proyecto sólida.



No se encuentra definido claramente y no se comunica las características de incidentes de seguridad potenciales.

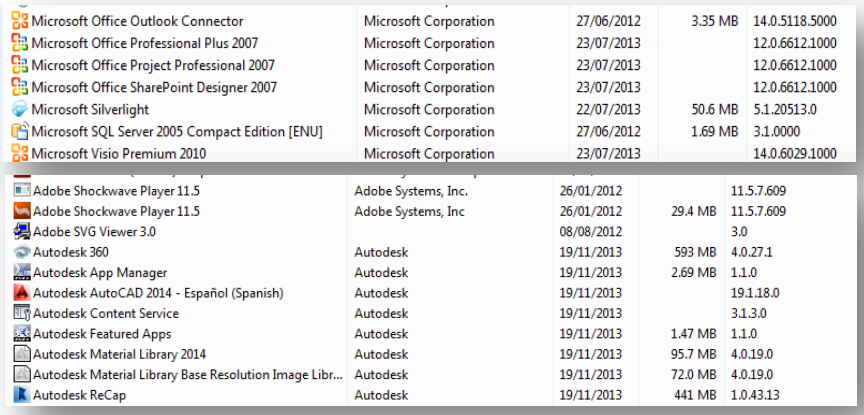


Ausencia de un marco de trabajo de continuidad de TI para soportar la continuidad del negocio.



No cumplen con los requisitos legales de seguridad referidos al diseño, operación, uso y gestión de los sistemas de información.

7.2.7 **HALLAZGOS**

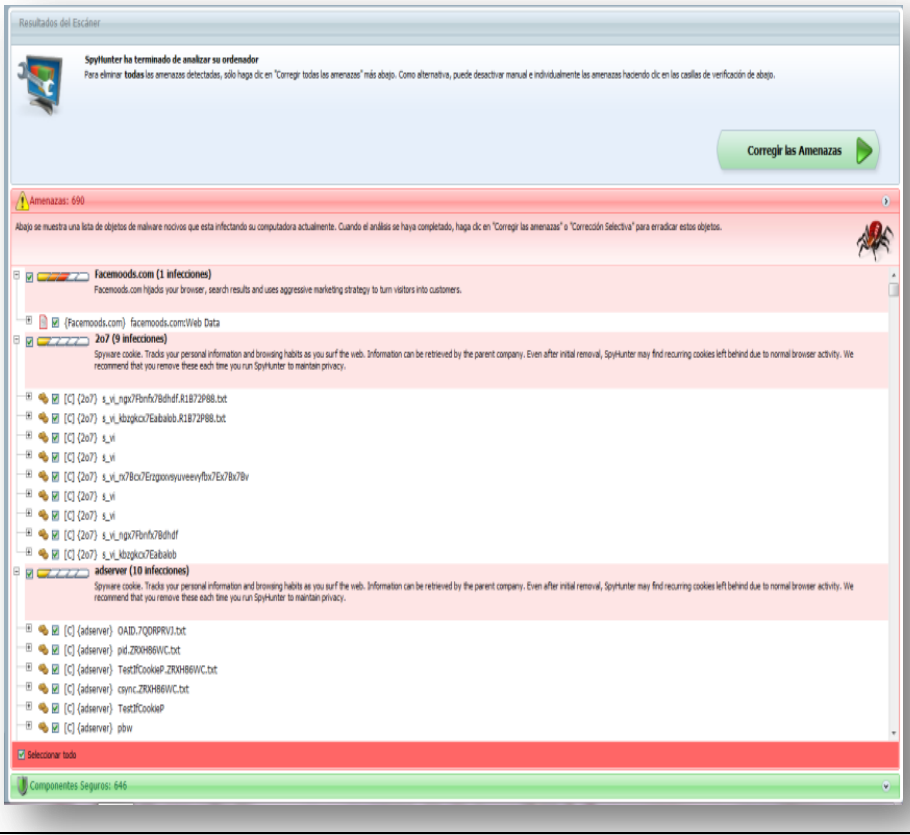
<table>
<tr><th>No.</th><th>Fecha</th><th>Prioridad</th><th>Escenario</th><th>Norma Aplicables</th></tr>
<tr><td>1</td><td>11/01/2014</td><td>Alta</td><td>Legal: Cumplimiento Regulatorio</td><td>Art. 47 de la Ley 222 de 1995, modificado por el Art. 1° de la Ley 603 de 2000
COBIT® 4.1 AI5.1, AI5.4</td></tr>
<tr><td>Hallazgo</td><td colspan="4">El listado de programas a continuación, representa el 90% aprox. del software instalado y en uso en CONTECSA
▪ Microsoft Office® Professional 2007 (22)
▪ Microsoft Windows® (19)
▪ Microsoft Visio® 2010 (10)
▪ AutoCAD® (12)
▪ Acrobat Professional® (22)</td></tr>
<tr><td>Set de Pruebas</td><td colspan="4">Se revisaron todos los equipos de usuario final. Una de las actividades fue relacionar los programas instalados, para luego ser cotejado con las licencias adquiridas.</td></tr>
<tr><td>Evidencias</td><td colspan="4"> 

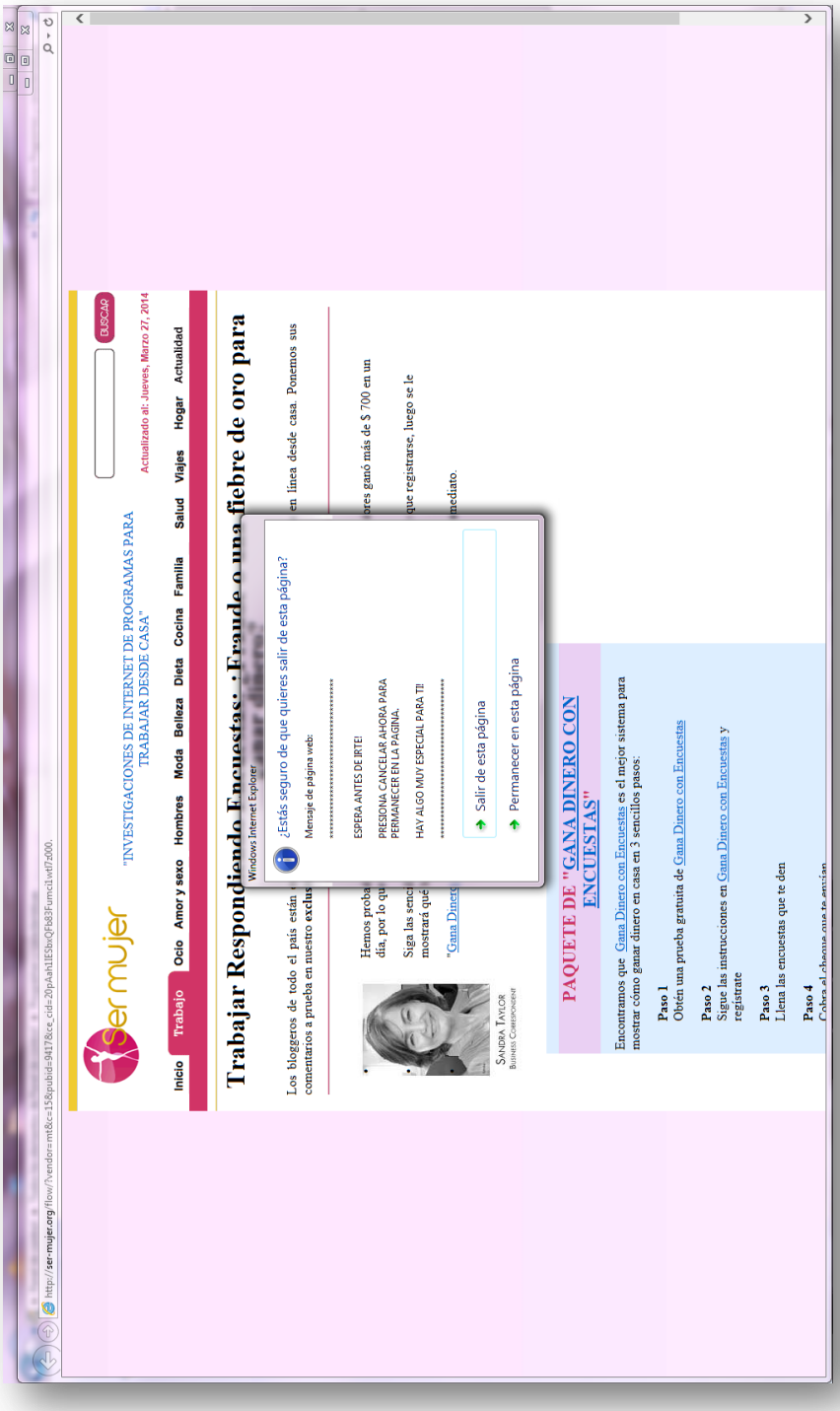
Printscreen de los programas instalados en los equipos

No se evidenciaron facturas de las licencias de los programas instalados en los equipos.</td></tr>
<tr><td>Riesgo</td><td colspan="4">Incumplimiento Regulatorio Legal sobre la Propiedad Intelectual y Derechos de Autor.

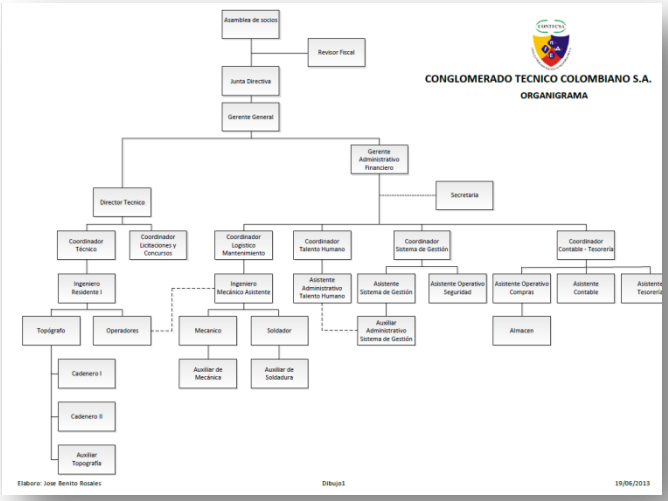
Causa(s):

▪ No existe un plan de adquisición de software.
▪ No existe restricción para las instalaciones en los equipos de usuario final.</td></tr>
<tr><td>Recomendaciones</td><td colspan="4">• Realizar un estudio sobre las necesidades de aplicaciones de los usuarios.
• Desarrollar y aplicar procedimientos de adquisición de TI que satisfagan los requerimientos del negocio.
• Adquirir legalmente las licencias correspondientes.
• Implementar Políticas de manejo y uso sobre los recursos de TI
• Restringir los permisos de instalaciones sobre los equipos.</td></tr>
</table>

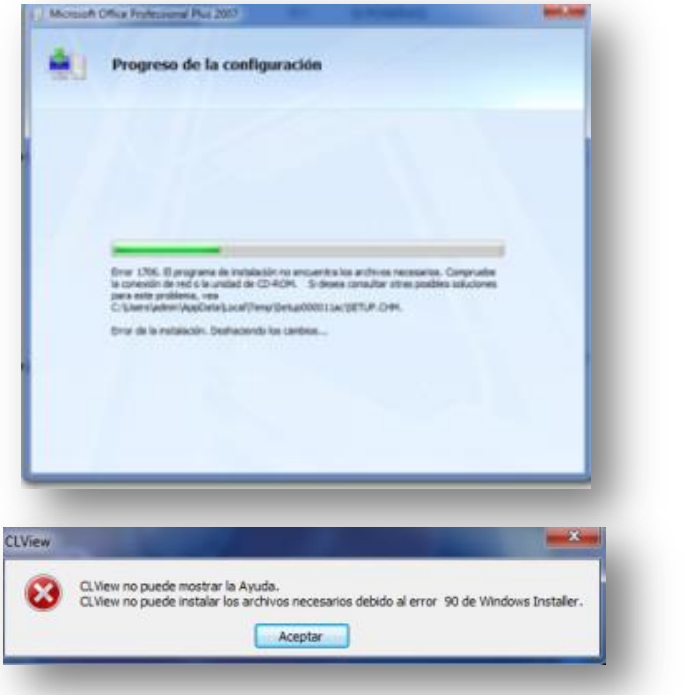
No.	Fecha	Prioridad	Escenario	Norma Aplicables
2	13/01/14	Alta	Ambiente de Control	COBIT® 4.1 PO6.3, PO7.2; DS54, DS5.10 ISO27001 5.2.1; ISO27001 5.2.2
Descripción	• Ausencia de políticas de seguridad definidas que apoyen la estrategia de TI. Es decir, que normalicen el hacer de los usuarios de los servicios informáticos ofrecidos en la empresa, y que a su vez, permitan establecer seguridad y de conciencia sobre el riesgo y su mitigación a través de un ambiente de control. • Se detectó la ejecución súbita de programas de dudosa procedencia.			
Set de Pruebas	• Al solicitarse las políticas de seguridad no se evidenció su existencia. Al revisar la configuración de los usuarios, se encontró que tienen privilegios administrativos por defecto, lo que sugiere ausencia de control en los usuarios finales. • Se revisaron todos los equipos de usuario final. Una de las actividades instalar un programa (SPyHunter) para identificar la instalación de malware en los equipos.			
Evidencias	Print Screen del listado de malware detectado a través de la aplicación SpyHunter 			

	Ventanas emergentes que se activan súbitamente. Se relacionan con la existencia de malware en los equipos. 

Riesgo	**1. Fraude Electrónico** **2. Ataques Informáticos** **3. Acceso no Autorizados a la Red Interna** **4. Falta de Disponibilidad, Confidencialidad e Integridad de la Información.** **Causas(s)** • No existe concientización sobre el riesgo y su impacto. • La Gerencia es reactiva al resolver los requerimientos de un ambiente de control. • Ausencia de un firewall (cortafuegos) físico o lógico. • Perfiles administrativos por defecto. • No se encontró software antivirus en los equipos.
Recomendaciones	• La Gerencia debe asumir la responsabilidad de proporcionar recursos para la implementación y divulgación de un ambiente de control que promocione las buenas prácticas internas en la empresa. • Definir e implementar políticas de seguridad de TI. • La Gerencia debería asegurar que todo el personal al que se le asigne responsabilidades o que participa en TI sea competente para realizar las tareas asignadas. • Es oportuno controlar el tráfico (entrante y saliente) de la información en la red. • Se debe activar el firewall en las conexiones de red.

No.	Fecha	Prioridad	Escenario	Normas Aplicables
3	23/11/2013	Alta	Gobierno (Gestión) de TI	COBIT® 4.1 PO1, PO4; Itil ®
Descripción	Administración inadecuada para la gestión de los recursos de TI.			
Set de Pruebas	• Se revisó el organigrama institucional. • Se analizó las respuestas obtenidas en las entrevistas, especialmente la realizada al encargado las actividades de adquisición de tecnología.			
Evidencias	 Organigrama en CONTECSA			
Riesgo	**1. Deficiencia en los Servicios y/o Infraestructura en TI.** **2. Medición no Confiable y por ende, Irrelevancia del Indicador costo-beneficio de la Tecnología.** **Causa(s):** • La ausencia de un área o departamento encargado de los procesos TI • Inexistencia de un plan estratégico de TI. • La realización de los proyectos de TI obedecen casi en su totalidad a un modo reactivo más que una estrategia organizacional.			
Recomendaciones	• Concientización e intervención de la alta gerencia para la alineación de los objetivos de TI con los objetivos del negocio. • Definir un Plan Estratégico para TI. • Ubicar a TI dentro de la estructura organizacional. Definición de Roles y Funciones. • Desarrollar prácticas adecuadas de supervisión dentro de la función de TI. • Implementar una metodología para la identificación y evaluación de soluciones TI, cuyo objetivo equilibre las necesidades de la organización en tiempo y costo.			

No.	Fecha	Prioridad	Escenario	Norma Aplicables
4	30/11/2013	Alta	Adquisición de Recursos TI	COBIT® 4.1 AI5 ISO27001
Descripción		La especificación de los acuerdos contractuales de las partes involucradas sobre el desarrollo de la aplicación SICON en la mayoría de ocasiones es verbal. Este tipo de relación contractual está definida por la confianza entre las partes por lo que se maneja informalmente.		
Set de Pruebas		Al solicitarse el contrato entre CONTECSA y el programador de la aplicación SICON no se evidenció su existencia.		
Evidencias		Testimonial Resultado de las entrevistas practicadas.		
Riesgo		**Incumplimiento de acuerdos en Proyectos de TI** **Causa:** • Procedimientos informales para la contratación de servicios.		
Recomendaciones		• Generar procedimientos para establecer, modificar y concluir contrato que apliquen a los proveedores. • Implementar prácticas para la selección de proveedores. • Realizar un contrato con el proveedor por el tiempo o los módulos que se encuentren pendientes		

No.	Fecha	Prioridad	Escenario	Norma Aplicables
5	13/01/2014	Alta	Aplicaciones	COBIT® 4.1 AI3.3, AI5 ISO27001
Descripción		Se detectaron errores de inicio en la herramienta ofimática Microsoft Office en algunos de los equipos de usuario final. Las actualizaciones críticas en la mayoría de los sistemas operativos y antivirus, no estaban al día.		
Set de Pruebas		Se revisaron todos los equipos de usuario final. Una de las actividades fue evaluar los programas utilizados con mayor frecuencia por los usuarios.		
Evidencias		 Print Screen de los mensajes emergentes al usar las aplicaciones de Office		
Riesgo		**1. Deficiencia en los Servicios y/o Infraestructura en TI.** **2. Insatisfacción del Cliente Interno de los servicios de TI.** **Causas(s)** • Inexistencia de un plan de mantenimiento. • La ausencia de personal asignado para ejecutar actividades básicas de actualización y control en los equipos de usuario final. • Uso de aplicaciones piratas.		
Recomendaciones		• Desarrollar prácticas adecuadas de supervisión dentro de la función de TI. • Instalar aplicaciones licenciadas que garanticen las actualizaciones liberadas por los proveedores.		

No.	Fecha	Prioridad	Escenario	Norma
6	12/02/2014	Alta	Aplicaciones	COBIT® 4.1 AI7.2
Descripción	La aplicación SICON está aún en etapa de desarrollo, sin embargo, la mayoría de sus módulos operativos están activos, por lo tanto, es oportuno que existan controles que generen, confiabilidad, disponibilidad y trazabilidad para minimizar la ocurrencia de eventos no deseados relacionados a este tipo de vulnerabilidad.			
Set de Pruebas	Se ingresó al sistema, se escogió la opción cambiar contraseña y se encontró que la validación activa no es efectiva, pues solicita digitar la contraseña actual como condición para efectuar el cambio de contraseña y aunque se digite de forma incorrecta ejecuta el cambio satisfactoriamente.			
Evidencias				
Riesgo	**Falta de Disponibilidad, Confidencialidad e Integridad de la Información.** **Causa** • Ausencia de un plan de pruebas estructurado.			
Recomendaciones	• Diseñar un plan de pruebas que abarque aspectos relevantes como la instalación, migración, conversión y aceptación de la aplicación. • Es oportuna una acreditación formal de las actualizaciones que se implementen.			

No.	Fecha	Prioridad	Escenario	Norma
7	13/02/2014	Alta	Documentación	COBIT® 4.1 AI4, PO7.5, PO7.5
Descripción		Los manuales de usuario final de la Aplicación SICON, así como los de sistema no han sido generados aun. El menú de ayuda en la aplicación SICON genera error. Lo anterior, obedece a que se optó por la terminación completa de la aplicación para luego, generar las guías y ayudas finalizado el desarrollo total del programa, lo que eventualmente puede obstaculizar la operación y el uso de los recursos.		
Set de Pruebas		1. Testimonial Resultado de las entrevistas practicadas. 2. Se ingresó a la aplicación y se revisó el menú ayuda identificado con el símbolo interrogación, obteniendo como resultado una página de error.		
Evidencias		 Print Screen del resultado de ingresar a la opción Ayuda de la aplicación SICON		
Riesgo		**Base y/o Guías de Conocimientos Focalizadas.** **Causa(s)** • Omisión de la importancia en mantener guías actualizadas que minimicen la dependencia sobre individuos clave. • Informalidad en los procedimientos de entrenamiento y/o capacitación.		
Recomendaciones		• Implementar una adecuada segregación de funciones. • Generar procedimientos de captura de conocimiento (documentación).		

No.	Fecha	Prioridad	Escenario	Norma
8	13/02/2014	Alta	Respaldo	ISO22301
Descripción	Aunque en el servidor tenga un disco duro espejo para respaldar la información en la base de datos del programa SICON, no se encontró un plan de valoración de crecimiento de información, adicionalmente, en la estaciones de trabajo se maneja la información similar a un usuario doméstico, es decir, no existe una concientización de realizar copias de seguridad de la información. La estructura de la información es a criterio de los usuarios, en muchos casos no se clasifica claramente la naturaleza de la información (personal o de la empresa) en los discos duros.			
Set de Pruebas	Se revisaron todos los equipos de usuario final. Una de las actividades fue evaluar la ubicación de los documentos.			
Evidencias	1. Testimonial Resultado de las entrevistas practicadas. 2. Revisión de las estaciones de trabajo.			
Riesgo	**Falta de Disponibilidad, Confidencialidad e Integridad de la Información** **Causa(s)** • Inexistencia de políticas de seguridad, específicamente las relacionadas al respaldo de información. • Desestimación de la probabilidad de ocurrencia por pérdida súbita de información relevante.			
Recomendaciones	• Implementar una política de respaldo y recuperación de información adecuada, • Generar ambientes para hacer pruebas de recuperación. • Fomentar la concientización de seguridad de la información.			

7.2.8 ANÁLISIS DE RIESGOS

El rol de TI en ha ido evolucionando, hoy día además de ser un área de soporte para la organización, con una eficiente administración, permite ventajas competitivas, es decir, más que un costo adicional representa un factor estratégico para la organización.

La importancia del Análisis de Riesgos obedece a que es una herramienta que nos permitirá identificar las amenazas a las que se encuentran expuestos los activos informáticos, estimar la frecuencia de materialización de tales amenazas y valorar el impacto que supondría en la empresa esa materialización. La norma ISO/IEC 27005 proporciona directrices para la gestión de riesgos de seguridad de la información.

La gestión de riesgos en TI se puede definir como un enfoque estructurado que permite manejar la incertidumbre ante una posible amenaza, a través de unas actividades proactivas definidas por la posición de la gerencia ante la posible materialización de un riesgo. Esta posición puede ser, aceptarlos, mitigarlos, transferirlos.

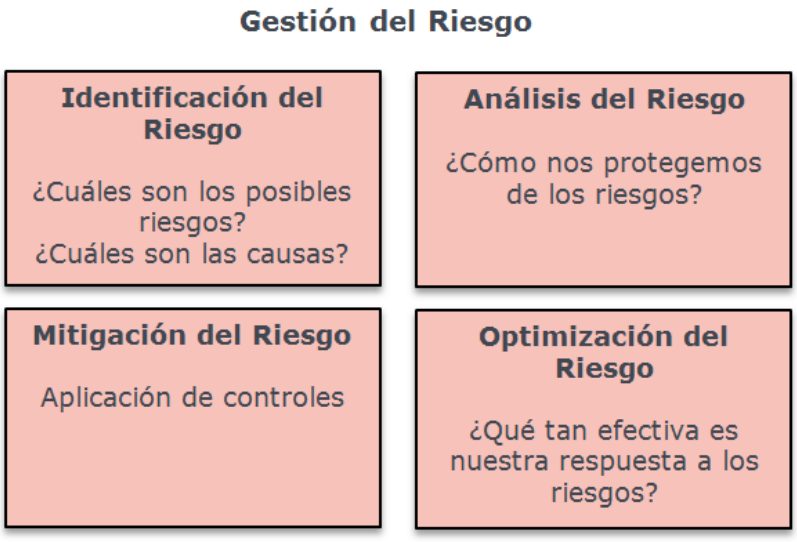


Figura 7. Ciclo de vida de la Gestión del Riego

7.2.8.1 **Escenarios de Riesgos**

Los riesgos son ocasionados por fallas y estas a su vez, se relacionan a un entorno. En este punto, relacionamos el entorno o escenario para cada uno de los riesgos asociados los hallazgos obtenidos durante esta investigación.

- ✓ Adquisición de Recursos TI
- ✓ Ambiente de Control
- ✓ Aplicaciones
- ✓ Documentación
- ✓ Legal
- ✓ Gobierno (Gestión) de TI
- ✓ Respaldo

7.2.8.2 **Riesgos Identificados**

ISACA®[16] define el riesgo de TI como *"el riesgo de negocio asociado con el uso, propiedad, operación, participación y adopción de TI en una empresa"*. A continuación los principales riesgos identificados, asociados al proceso de TI en CONTECSA:

- ✓ **Acceso no autorizado a la red Interna:** La ausencia de un firewall que controle el tráfico de información entrante y saliente, así como los permisos administrativos activos por defecto de los usuarios finales en las estaciones, genera un ambiente propicio para que usuarios sin autorización obtengan acceso a los equipos a través de Internet o de una red.

[16] Systems Audit and Control Association. Asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades auditoría y control en sistemas de información

- ✓ **Ataques Informáticos**. Existen muchos tipos de ataque informáticos, entre ellos podemos mencionar: desestabilizar el sistema, denegación de servicios, robo de información, entre otros.

- ✓ **Bajo nivel de utilización de las TI como ventaja competitiva**. La utilización de las tecnologías de la información en la actualidad permiten mantener una imagen corporativa actualizada, además, amplían el acceso a los clientes actuales y futuros y viceversa.

- ✓ **Base y/o Guías de Conocimientos Focalizadas**. Existen funcionarios puntales que tienen el conocimiento de cambios y ejecución relevantes en la organización, al no haber documentación detallada como por ejemplo, manuales no se puede impartir un adecuado empalme o capacitación en el evento de la ausencia de dichas personas.

- ✓ **Pérdida de la Información**. La desestimación de este riesgo es la principal causa para no tener en cuenta el evento en que un daño súbito ocasione la pérdida de información crítica relevante para una determinada actividad, la falta de respaldos incrementa la incertidumbre.

- ✓ **Desempeño Operacional Inadecuado de la Infraestructura de TI.** La ausencia de actividades de administración maximiza la proliferación de anomalías, que se convierten en vulnerabilidades por ejemplo, desactualizaciones, daños físicos, incompatibilidades.

- ✓ **Falta de Disponibilidad, Confidencialidad e Integridad de la Información.** La información es el principal patrimonio de una organización, por lo que su protección y seguridad resulta imprescindible. La capacidad de que esté siempre disponible, que sea conocida únicamente por las personas autorizadas y que su contenido permanezca inalterado – salvo una modificación por el personal autorizado- requiere de acciones puntuales que minimicen la de ocurrencia de este riesgo.

- ✓ **Fraude Electrónico**. Dada la vulnerabilidad que precisa el hecho de no existir un firewall, incrementa la probabilidad de ocurrencia de esta modalidad de ataque informático, en donde la suplantación de identidad se enfatiza para la adquisición de información bancaria y tarjetas de crédito.

- ✓ **Inadecuada Gestión de Proveedores de TI.** La gestión de proveedores se ocupa de formalizar la relación con los suministradores de servicios de los que depende la organización en TI, el objetivo principal es alcanzar mayor calidad a un precio adecuado entre estas actividades se encuentran: identificación de nuevos proveedores, definición y negociación de nuevos contratos, renovar y terminar contratos. Adicionalmente, mantener actualizada y disponible la información relacionada de los proveedores y los servicios que prestan.

- ✓ **Inadecuado cumplimiento del Gobierno de TI**. El gobierno de TI es efectivo siempre y cuando se determinen las actividades y los riesgos que requieran ser administrados. Identificar la manera en que TI puede contribuir al logro de los objetivos del negocio, implementar las soluciones y monitorearlas son las actividades que garantizan un buen gobierno de TI.

- ✓ **Incumplimiento Regulatorio Legales**. La Dirección de Impuestos y Aduanas Nacionales – DIAN, está facultada para verificar el estado de cumplimiento de las normas sobre derecho de autor e impedir que a través de su violación se evadan tributos. Las sociedades comerciales tienen la obligación de presentar informes de gestión en los cuales debe consignarse el cumplimiento de las normas sobre propiedad intelectual y derechos de autor. El incumplimiento podría generar sanciones hasta 8 años de cárcel y multa de hasta 1000SMLV, lo cual podría afectar la imagen de la compañía.

- ✓ **Incumplimiento de acuerdos en proyectos de TI**. La informalidad de los procesos y el no contar con un contrato donde se detallen los acuerdos donde incrementa el riesgo por incumplimiento de términos y acuerdos.

- ✓ **Indeterminabilidad de Acciones y Responsabilidades (No Trazabilidad).** La no existencia de logs, ni registros de acciones en las actividades relacionadas a TI en general, pueden generar que no haya un seguimiento oportuno que conlleven hacía las fallas que ocasionen ciertos eventos no deseados.

- ✓ **Insatisfacción del Cliente Interno de los Servicios de TI.** La apreciación por parte de los usuarios de los recursos informáticos provistos por la empresa, es clave para la motivación al momento de desarrollar las actividades propias de su gestión. Asimismo, una infraestructura robusta genera un ambiente de seguridad y organización.

- ✓ **Lineamientos de TI no acordes con la estrategia del negocio.** Es clave que alinear TI con los objetivos del negocio, este vínculo asegura que TI genere beneficios y brinde un valor intrínseco, como lo es la ventaja competitiva y optimización de recursos.

- ✓ **Medición no confiable y por ende, Irrelevancia del Indicador Costo-Beneficio de la Tecnología**. Todo proceso en TI debería evaluarse de forma regular en el tiempo, en cuanto a su calidad y cumplimiento del requerimiento de control.

7.2.8.3 **Mapa de Riesgos TI**

Cumpliendo con el objetivo de esta Consultoría, que es el de proporcionar a la alta gerencia información relevante y que les permita la toma de decisiones estratégicas, a continuación describimos el mapa de riesgos identificados asociados al proceso de TI en CONTECSA.

Calificación	Probabilidad	Impacto
1	Improbable	Mínimo
2	Posible	Moderado
3	Probable	Mayor
4	Casi Certeza	Grave

Nivel de Riesgo (Probabilidad x Impacto)	
Menor a 4	**Bajo**
Igual a 4	**Moderado**
Mayor a 4	**Alto**

Figura 8. Valoración del Riesgo

	Riesgos Inherentes de TI en CONTECSA	RESIDUAL	
		Probabilidad Valores (1-4)	Impacto Valores (1-4)
R1	Acceso no autorizados a la red Interna	**4**	**4**
R2	Ataques informáticos	**4**	**4**
R3	Bajo nivel de utilización de la TI como ventaja competitiva	**3**	**2**
R4	Base y/o Guías de Conocimientos Focalizadas	**4**	**4**
R5	Desempeño operacional inadecuado de la infraestructura de TI (hardware, software, etc.)	**4**	**4**
R6	Falta de disponibilidad, confidencialidad e integridad de la información	**4**	**4**
R7	Fraude electrónico	**4**	**4**
R8	Inadecuada gestión de proveedores de TI	**2**	**3**
R9	Inadecuado cumplimiento del Gobierno TI	**4**	**4**
R10	Incumplimiento de acuerdos en proyectos de TI	**4**	**4**
R11	Incumplimientos regulatorios legales	**4**	**4**
R12	Indeterminabilidad de acciones y responsabilidades (No Trazabilidad)	**3**	**3**
R13	Insatisfacción del cliente interno de los servicios de TI	**3**	**3**
R14	Lineamientos de TI no acordes con la estrategia del negocio	**4**	**4**
R15	Medición no confiable y por ende, irrelevancia del indicador costo-beneficio de la tecnología	**4**	**3**
R16	Perdida de la Información	**4**	**4**

Tabla 3. Mapa de Riesgos

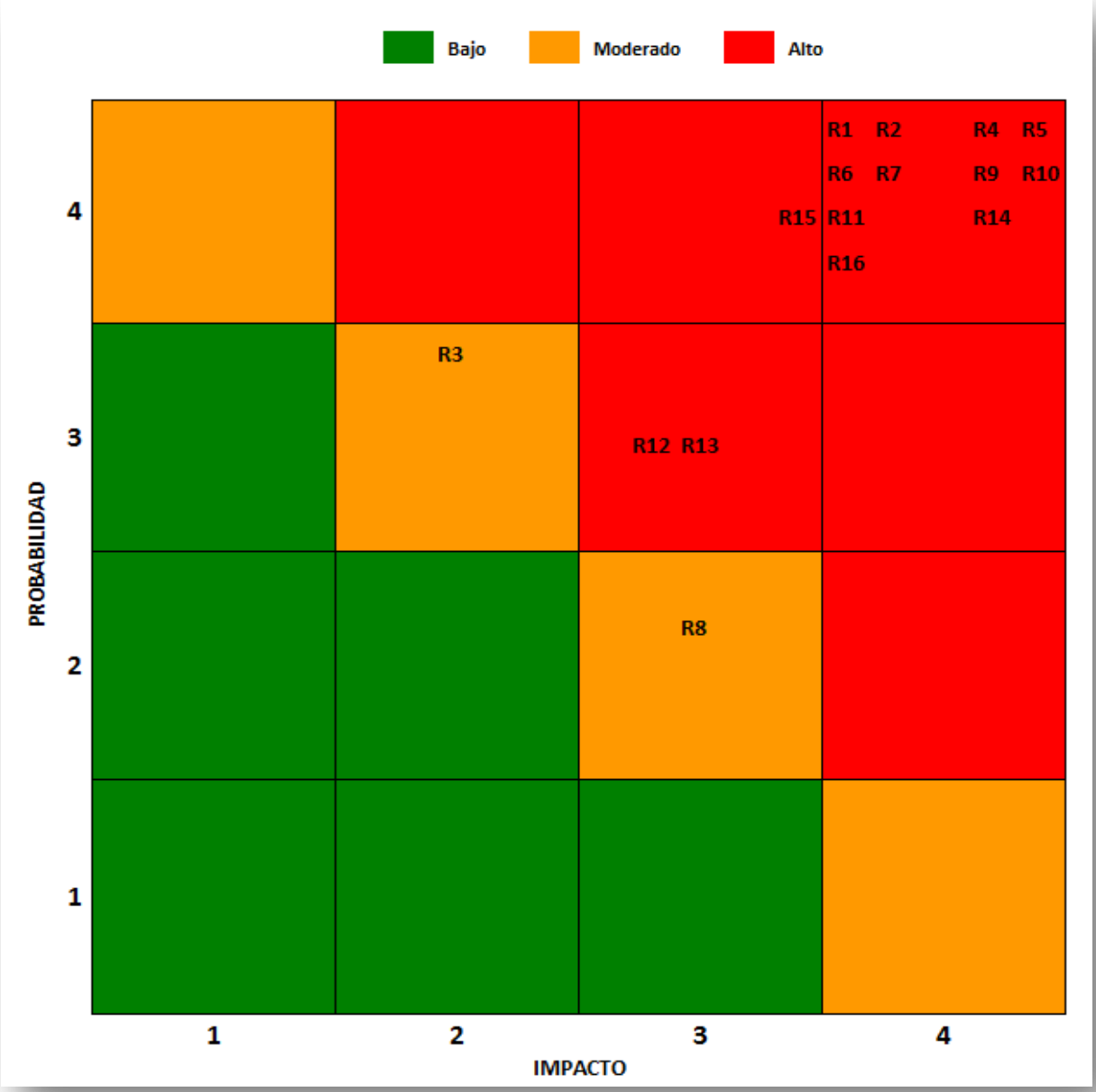


Figura 9. Riesgos - Probabilidad Vs Impacto

7.2.9 **CONTROLES**

Los controles son las acciones y medidas que se aplican con el objeto de minimizar la probabilidad de ocurrencia y la magnitud de impacto de un riesgo identificado.

- ✓ **Implementar un Sistema de Gestión de Seguridad de la Información SGSI**. Un SGSI es el diseño, implementación y mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, con el fin de asegurar criterios como la **confidencialidad**, **integridad** y **disponibilidad** de los activos de información, a su vez, **minimizar los riesgos** de seguridad de la información.

  Con la puesta en marcha de este control se disminuiría notablemente los riesgos identificados en esta Consultoría, debido a que este sistema abarcaría las causales de las vulnerabilidades a las que CONTECSA se encuentra actualmente expuesta.

  Del anterior se desprenden los siguientes controles:

  - Designar personal capacitado para atribuir la responsabilidad de administrar, mantener y dirigir los procesos de TI en la organización.
  - Generar y divulgar políticas de seguridad de la información clara y efectiva sobre el uso de los recursos informáticos.
  - Fortalecer las validaciones de acceso a los aplicativos.
  - Crear políticas y procedimientos para la administración de la BD del aplicativo SICON.
  - Generar procedimientos de los cambios que se realicen en la aplicación SICON.

- Generación y actualización de documentación relevante de los aplicativos en uso (manuales técnicos, usuario final e instalación).
- Capacitación a los usuarios sobre el uso correcto y administración de los aplicativos.
- Fortalecer y ampliar las Políticas de Respaldo.
- Desarrollar y aplicar procedimientos de adquisición de TI que satisfagan los requerimientos del negocio y de ley.
- Implementar prácticas para la selección de proveedores.
- Implementar firewall para controlar el tráfico (entrante y saliente) de la información en la red.
- Elaborar un contrato que se formalice las actividades y brinde a las partes interesadas, en el cual se definan principalmente propiedad intelectual del trabajo desarrollado, garantías, acuerdos a nivel de servicios.

7.2.10 MODELO DE MADUREZ DE COBIT®

El grafico correspondiente en el informe ejecutivo, se parametriza de acuerdo de la clasificación siguiente:

- ✓ **0 No existente**. Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.

- ✓ **1 Inicial.** Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques ad hoc que tienden a ser aplicados de forma

individual o caso por caso. El enfoque general hacia la administración es desorganizado.

- ✓ **2 Repetible.** Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.

- ✓ **3 Definido.** Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.

- ✓ **4 Administrado.** Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.

- ✓ **5 Optimizado.** Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

8. CONCLUSIÓN

Actualmente, la aplicación eficiente y efectiva de las buenas prácticas de TI en una organización facilita sus actividades misionales coadyuvando al logro de sus objetivos. Los marcos de referencias utilizados para evaluar la situación actual de TI en CONTECSA, así como, suministrar las recomendaciones pertinentes consignadas en los informes, permitieron cumplir con el objetivo de orientarlos hacía la mejora de sus procesos de TI, para que como organización estén más próximos de alcanzar sus metas de la mano de la tecnología.

La identificación de los riesgos sirvió como concientización del peligro y las recomendaciones a la aplicación de controles básicos para minimizarlos.

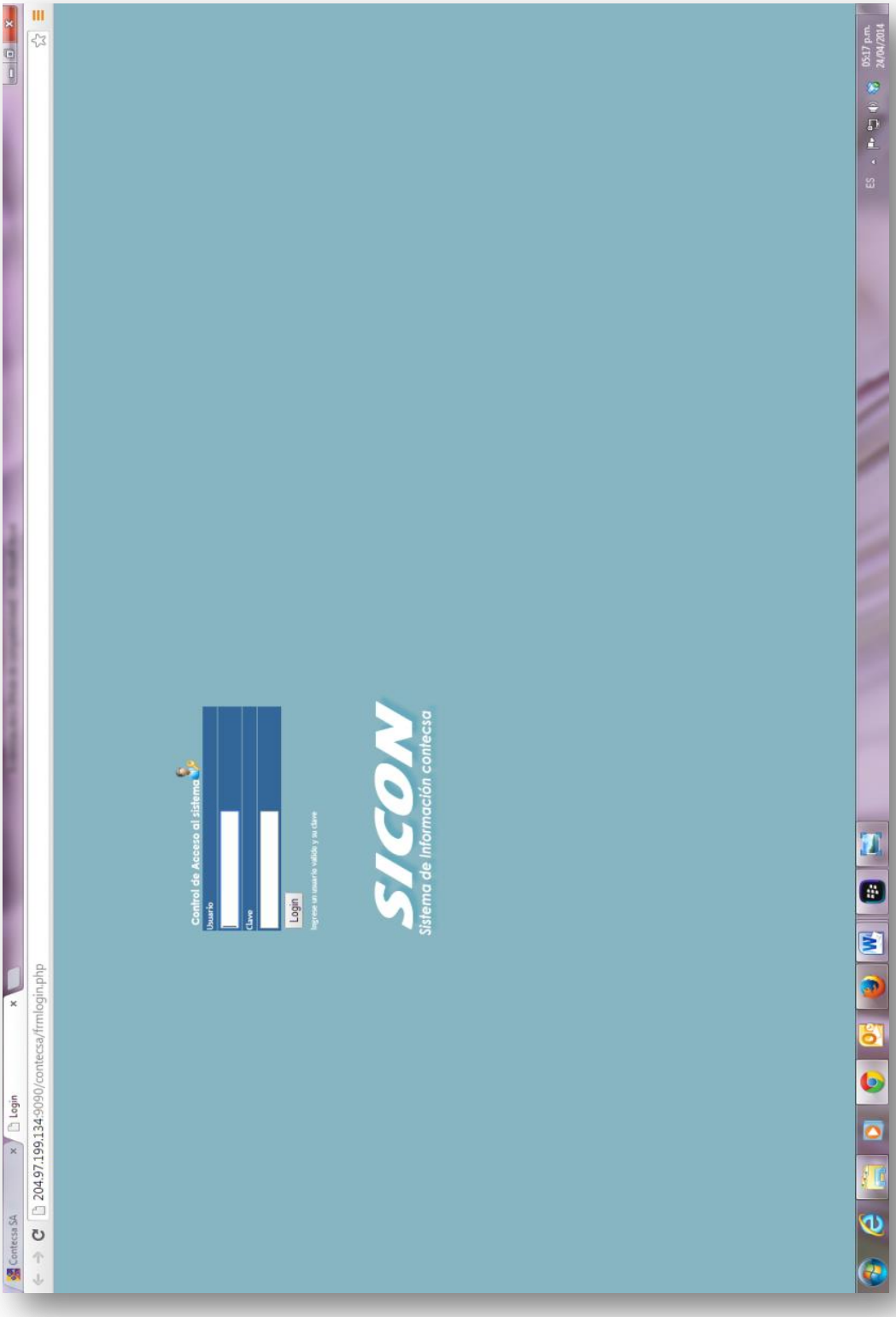
Esta Consultoría le ofreció a CONTECSA S.A. el conocimiento de los beneficios que pueden tener con el uso eficiente de los recursos de TI y con el ambiente de calidad que se está gestando, la información brindada es un gran aporte para la toma de decisiones que sin duda se reflejará factores críticos como de gestión y económico.

9. BIBLIOGRAFIA

- ✓ Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit. 2008 IT Governance Institute.
- ✓ Directrices Gerenciales Julio de 2000 3ra Edición. Publicado por El Comité de Dirección de COBIT y el IT Governance InstituteTM.
- ✓ IT Governance Institute Cobit 4.0.
- ✓ Directrices OCDE para la seguridad de sistemas y redes de información. Hacia una cultura de la seguridad. París: OCDE, Julio de 2002.
- ✓ Auditoria de la Información. Identificar y explotar la información en las Organizaciones, Cristina Soy i Aumatell Noviembre 2012 1ra edición.
- ✓ Auditoria Informática, Gonzalo Alonso Rivas. 1988 Ediciones Díaz de Santo, S.A.
- ✓ Estándar Internacional ISO, 27001 15 Octubre 2005 1ra edición.
- ✓ Auditoria de Sistemas, Una visión práctica. 2001 Universidad Nacional de Colombia – Manizales.
- ✓ Norma Técnica Colombiana NTC 1486 (sexta Actualización)
- ✓ Normas para la Entrega de Tesis y Trabajos de Grado a la Unidad de Información (Ver. 2 Junio 2012)
- ✓ Norma ISO 22301 Continuidad del Negocio
- ✓ Norma ISO 31000 Riesgos
- ✓ http://www.inteco.es/glossary/Formacion/Glosario/COBIT
- ✓ http://www.noguerakrb.net/index.php/component/content/article/25-the-project/46-cobitr
- ✓ http://www.iso27000.es/download/doc_iso27000_all.pdf
- ✓ https://www.inteco.es/wikiAction/Seguridad/Observatorio/area_juridica_seguridad/Enciclopedia/Articulos_1/iso_27005_en
- ✓ http://www.isaca.org/Pages/Glossary.aspx

ANEXOS

Anexo A. Acceso al Programa SICON



Anexo B. Menú de Opciones Programa SICON

Anexo C. Equipos de Usuario Final.

	Usuario	CPU			MONITOR		TECLADO		IMP.		Sistema Operativo
		Procesador	DD	RAM	Marca	S/N	Marca	S/N	Marca	S/N	
1	Recepcionista	INTEL CORE 2 DUO	320 GB	2 GB	ACER	4021	ACER	B010	HP J3680	ZOMS	WIN 7 PRO
2	Gerente General	HP TODO EN UNO	1 TERA	8 GB	HP		HP	H62F	HP1006	4515	WIN.8
3	Gerente Financiero	DELL INTEL CORE I3	500 GB	4 GB	DELL	6627	DELL INA	0331	EPSON L335	8285	WIN. 7
4	Licitaciones	DELL INTEL CORE I3	500 GB	4 GB	DELL ALL IN ONE	4180	DELL INAM	0B0P	HP 5525	7193	WIN 7
5	Director Técnico	COREL I7	1 TERA	6 GB	LG	805	GENIUS	6799	-	-	WIN 7 ULTIMATE
6	Profesional	ACER AMD DUO CORE	500 GB	3 GB	HP	603X	HP	WONS	-	-	WIN 7 HOME BASIC
7	Profesional	HP DUO CORE	250 GB	2 GB	HP	60RR	HP	52VN	-	-	WIN 7 PRO
8	Talento Humano	COMPAQ AMD DUO CORE	500 GB	3 GB	ACER	4021	COMPAQ	7656	HP1006	7531	WIN 7 PRO
9	Auxiliar Contable 1	INTEL CORE 2 DUO	160 GB	2 GB	DELL	41MM	DELL	1813	-	-	WIN 7 PRO
10	Auxiliar Contable 2	QBEX DUAL CORE	1 TERA	4 GB	QBEX	959	QBEX	5738	EPSONFX890	7123	WIN 7 HOME BASIC
11	Contador	DELL INTEL CORE I5	1 TERA	6 GB	DELL	4180	DELL INAM	4751	HP LASERJET	HOLQ	WIN 7 HOME PRE
12	Compras	COMPAQ AMD	500 GB	2 GB	COMPAQ	059C	COMPAQ	M2P0	-	-	WIN 7 PRO
13	Juridica	COMPAQ DUO CORE	320 GB	2 GB	COMPAQ	6042	COMPAQ	WONF	-	-	WIN VISTA
14	Profesional	HP COMPAQ DUO CORE	320 GB	2 GB	COMPAQ	QNFG	GENIUS	7775	-	-	WIN 7 PRO
15	Profesional	DELL CORE 2 DUO	320 GB	1 GB	DELL	0HGS	GENIUS	6799	-	-	WIN 7 PRO
16	Almacen 1	DELL INTEL CORE 2 DUO	500 GB	2 GB	SAMSUNG	188L	ACER	100	-	-	WIN 7 PRO
17	Almacen 2	HP COMPAQ DUO CORE	320 GB	2 GB	ACER	8343	ACER	K701	-	-	WIN 7 PRO
18	Almacen 3	ACER DUO CORE	640 GB	2 GB	HP	603T	GENIUS	1709	-	-	WIN 7 PRO
19	Área Técnica	ACER DUO CORE	640 GB	4 GB	ACER	2140	ACER	100	HP1006	4530	WIN 7 PRO
20	Topografia	LENOVO CORE I3	1 TERA	4 GB	LENOVO	846	LENOVO	6443	-	-	WIN 7 HOME BASIC
21	Área Técnica 2	LENOVO CORE DUO	500 GB	3GB	LENOVO	405	GENIUS	7774	-	-	WIN 7 HOME BASIC
22	Ingenieria	DELL INTEL CORE I3	500 GB	4 GB	DELL	QUES	DELL	1616	-	-	WIN 7 HOME BASIC

Anexo D. Carta de Autorización.

CONTECSA

NIT. 802.005.436-1

Barranquilla, Julio 14 de 2.013

Señores:
UNIVERSIDAD DE LA COSTA – CUC
Atn.: Víctor Montaño Ardila – Coordinador Académico
Especialización en Auditoria a los Sistemas de Información

Ref.: **Carta de Aceptación Consultoría**

Cordial saludo.

Yo DIANA PATRICIA RODRIGUEZ ISIDRO, identificada como aparece al pie de mi firma, en calidad de GERENTE GENERAL de la empresa CONGLOMERADO TECNICO COLOMBIANO S.A. CONTECSA, manifiesto formalmente la aceptación de la PROPUESTA DE CONSULTORIA A LOS PROCESOS DE TECNOLOGÍA formulada por las Ingenieras Ana Molinares, Lenys Rangel y Manuela Villar, cuyo resultado tiene como objeto, coadyuvar al plan de MEJORAMIENTO CONTINUO DE LA CALIDAD Y LA PRODUCTIVIDAD que estamos implementando en nuestra organización. Solicito de igual forma, se inicie con los pasos necesarios, tales como la evaluación de la empresa y otros que consideren pertinentes para que se dé inicio a la CONSULTORIA PROPUESTA.

Asimismo, me comprometo a suministrar la información necesaria que soliciten para que se lleve a buen término en forma y tiempo esta CONSULTORIA, bajo los acuerdos de confidencialidad establecidos.

Atentamente,

DIANA PATRICIA RODRIGUEZ ISIDRO
CC: 22.668.761 de Barranquilla

Oficina Principal Barranquilla: Carrera 57 No. 68 - 94 • Teléfonos: 357 9898 - 357 9988
Sede Puerto Colombia: Km. 98 + 600 Vía al Mar, Entrada Antorcha • Celular: 318 813 4420

Anexo E. Acuerdo de Confidencialidad.

CLAUSULAS:

PRIMERA: En virtud del presente acuerdo, LOS CONSULTORES, se obligan a no divulgar, revelar, exhibir, mostrar, comunicar utilizar y/o emplear en su favor o en favor de terceros la información confidencial que reciban de LA EMPRESA en el territorio nacional o fuera de este, durante la vigencia de la consultoría y después del término de ésta, y en consecuencia mantenerla de manera confidencial y privada, y proteger dicha información para evitar su divulgación no autorizada.

SEGUNDA: LOS CONSULTORES se encuentran en la obligación de no revelar la información recibida, a terceros con el fin de dañar y denigrar la imagen institucional de LA EMPRESA. En cuyo caso, LA EMPRESA se encontrará facultada a exigir el pago por la indemnización de los daños y perjuicios ocasionados.

TERCERA: La información confidencial, será en todo momento y continuará siendo propiedad de LA EMPRESA. LOS CONSULTORES acuerdan no hacer uso de la información confidencial, excepto para el desarrollo y finalidad de la consultoría.

CUARTA: Perderá el carácter de información confidencial, y por ende no estará sometida a lo señalado en este acuerdo, aquella: (a) Información que al momento de recepción por parte de LOS CONSULTORES sea de dominio público; o (b) Información que haya sido adquirida directa o indirectamente de una fuente totalmente independiente de alguna de las partes aquí comprometidas.

QUINTA: Las partes convienen que en caso de que LOS CONSULTORES incumplan parcial o totalmente con las obligaciones del presente acuerdo, éstos serán responsables de los daños y perjuicios que ocasionen.

SEXTA: LOS CONSULTORES están en la obligación de devolver la información confidencial a la que se ha tenido acceso en el momento que termine la consultoría, estableciendo, igualmente, que a pesar de dicha terminación, la obligación de confidencialidad y secreto permanecerá vigente durante el plazo que sea establecido por las partes.

SEPTIMA: Toda la información que llegue a conocerse como resultado de la ejecución de la consultoría no puede ser divulgada, comercializada, utilizada, ni revelada a terceros con fines distintos a los acordados por las partes. Cualquier violación a esta cláusula, permitirá a la parte afectada, iniciar acciones a que se refiere el Código Penal Colombiano.

OCTAVA: Este Acuerdo se regirá en todo aspecto por las leyes y los tribunales de la República de Colombia. El acuerdo ha sido escrito y cualquier negociación subsiguiente o controversias serán conducidas en español.

2

NOVENA: La vigencia del presente acuerdo en relación a las restricciones y obligaciones consagradas estarán vigentes desde el momento en que sea recibida la información por un periodo de un (1) año.

DECIMA: El presente acuerdo solo se entenderá perfeccionado con la firma de ambas partes, quedando regulados los acuerdos verbales anteriores que pudiesen existir.

Para constancia de lo anterior, se firma en Barranquilla a los veinticuatro (24) días del mes de Septiembre del 2.013, en dos ejemplares de igual tenor con destino a cada una de las partes.

LA EMPRESA,

DIANA PATRICIA RODRIGUEZ ISIDRO
CC: 22.668.761 de Barranquila
Gerente General
CONGLOMERADO TECNICO COLOMBIANO S.A. - CONTECSA

LOS CONSULTORES,

ANA MARÍA MOLINARES
CC: 22.479.853 de Barranquilla

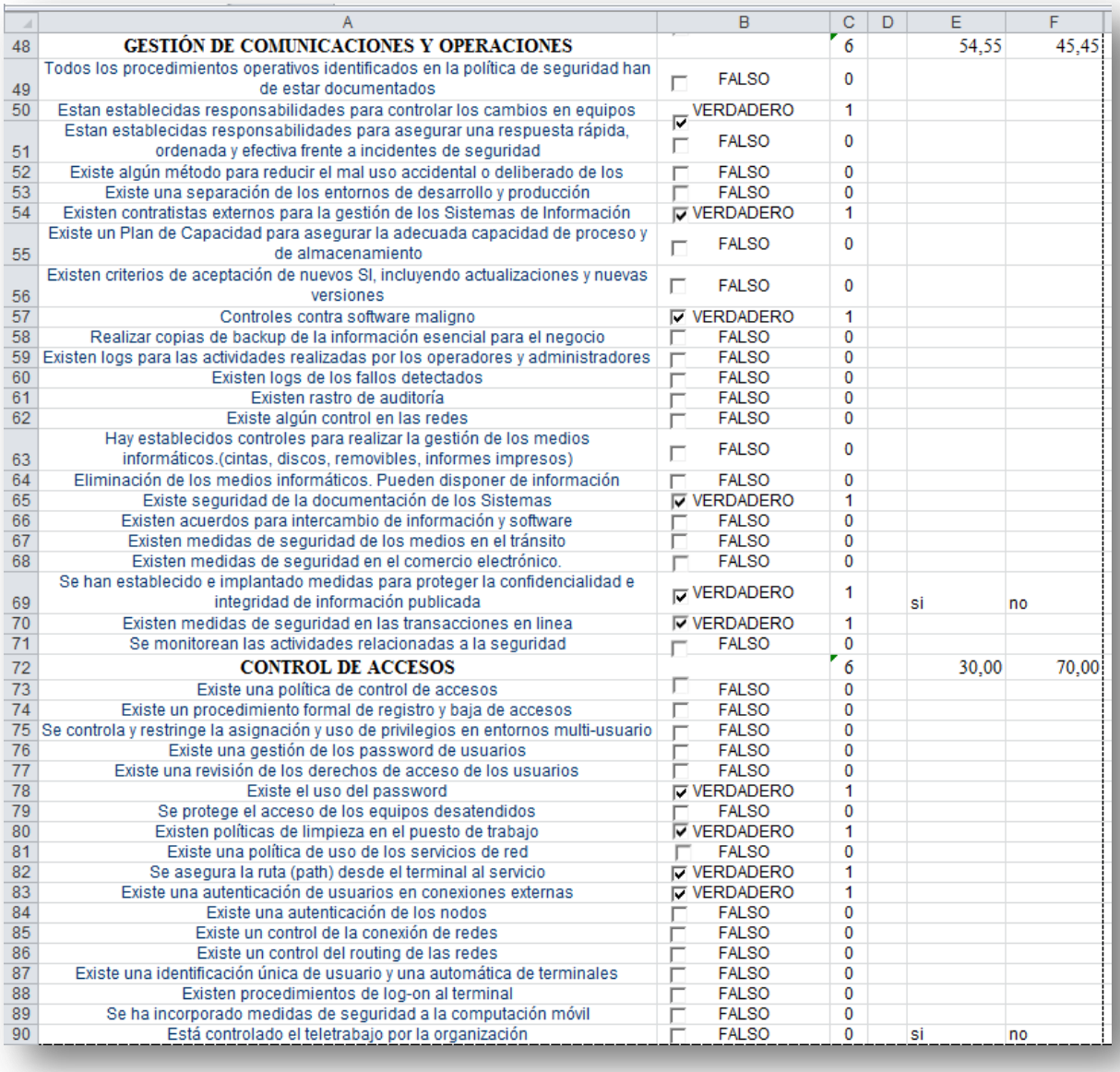
LENYS RANGEL FERRER
CC: 55.230.510 de Barranquilla

MANUELA VILLAR ÁVILA
CC: 1.045.671.412 de Barranquilla

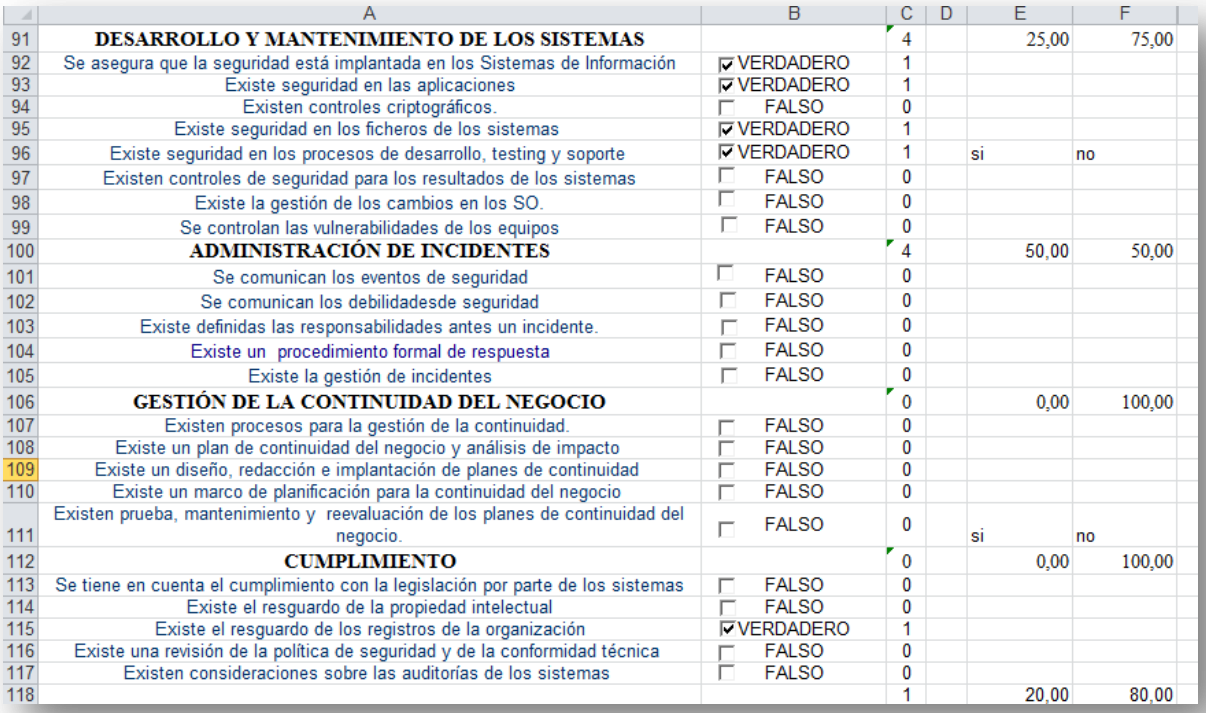
Anexo F. Diagnóstico ISO 27001

A través de una hoja de cálculo se realiza este check list de los principales puntos que trata la norma ISO 27001, este fue el resultado para la empresa objeto de la consultoría y es la base para los gráficos en el informe detallado en la sección de Análisis e Interpretación.

	A	B	C	D	E	F
1	**FORMULARIO PARA AUTODIAGNÓSTICO**					
2	**(ISO 27001)**					
3	**POLÍTICAS DE SEGURIDAD**					
4	•Existen documento(s) de políticas de seguridad de SI	☐ FALSO	0			
5	•Existe normativa relativa a la seguridad de los SI	☐ FALSO	0			
6	•Existen procedimientos relativos a la seguridad de SI	☐ FALSO	0			
7	•Existe un responsable de las políticas, normas y procedimientos	☐ FALSO	0			
8	•Existen mecanismos para la comunicación a los usuarios de las normas	☐ FALSO	0			
9	•Existen controles regulares para verificar la efectividad de las políticas	☐ FALSO	0		si	no
10	**ORGANIZACIÓN DE LA SEGURIDAD**		0		0,00	100,00
11	•Existen roles y responsabilidades definidos para las personas implicadas en la seguridad	☐ FALSO	0			
12	•Existe un responsable encargado de evaluar la adquisición y cambios de SI	☑ VERDADERO	1			
13	La Dirección y las áreas de la Organización participa en temas de seguridad	☐ FALSO	0			
14	•Existen condiciones contractuales de seguridad con terceros y outsourcing	☐ FALSO	0			
15	•Existen criterios de seguridad en el manejo de terceras partes	☐ FALSO	0			
16	•Existen programas de formación en seguridad para los empleados, clientes y terceros	☐ FALSO	0			
17	•Existe un acuerdo de confidencialidad de la información que se accesa.	☐ FALSO	0			
18	•Se revisa la organización de la seguridad periódicamente por una empresa	☐ FALSO	0		si	no
19	**ADMINISTRACIÓN DE ACTIVOS**		1		12,50	87,50
20	•Existen un inventario de activos actualizado	☑ VERDADERO	1			
21	•El Inventario contiene activos de datos, software, equipos y servicios	☑ VERDADERO	1			
22	•Se dispone de una clasificación de la información según la criticidad de la misma	☑ VERDADERO	1			
23	• Existe un responsable de los activos	☑ VERDADERO	1			
24	•Existen procedimientos para clasificar la información	☐ FALSO	0			
25	•Existen procedimientos de etiquetado de la información	☐ FALSO	0		si	no
26	**SEGURIDAD DE LOS RRHH**		4		66,67	33,33
27	•Se tienen definidas responsabilidades y roles de seguridad	☐ FALSO	0			
28	•Se tiene en cuenta la seguridad en la selección y baja del personal	☑ VERDADERO	1			
29	•Se plasman las condiciones de confidencialidad y responsabilidades en los	☐ FALSO	0			
30	•Se imparte la formación adecuada de seguridad y tratamiento de activos	☑ VERDADERO	1			
31	•Existe un canal y procedimientos claros a seguir en caso de incidente de	☐ FALSO	0			
32	•Se recogen los datos de los incidentes de forma detallada	☐ FALSO	0			
33	•Informan los usuarios de las vulnerabilidades observadas o sospechadas	☐ FALSO	0			
34	•Se informa a los usuarios de que no deben, bajo ninguna circunstancia, probar las vulnerabilidades	☐ FALSO	0		si	no
35	• Existe un proceso disciplinario de la seguridad de la información	☐ FALSO	0			
36	**SEGURIDAD FÍSICA Y DEL AMBIENTE**		2		22,22	77,78
37	Existe perímetro de seguridad física(una pared, puerta con llave).	☑ VERDADERO	1			
38	Existen controles de entrada para protegerse frente al acceso de personal no autorizado	☐ FALSO	0			
39	Un área segura ha de estar cerrada, aislada y protegida de eventos naturales	☐ FALSO	0			
40	En las áreas seguras existen controles adicionales al personal propio y ajeno	☐ FALSO	0			
41	Las áreas de carga y expedición están aisladas de las áreas de SI	☑ VERDADERO	1			
42	La ubicación de los equipos está de tal manera para minimizar accesos	☑ VERDADERO	1			
43	Existen protecciones frente a fallos en la alimentación eléctrica	☑ VERDADERO	1			
44	Existe seguridad en el cableado frente a daños e intercepciones	☑ VERDADERO	1			
45	Se asegura la disponibilidad e integridad de todos los equipos	☑ VERDADERO	1			
46	Existe algún tipo de seguridad para los equipos retirados o ubicados	☐ FALSO	0			
47	Se incluye la seguridad en equipos moviles	☐ FALSO	0			



	A	B	C	D	E	F
48	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**		6		54,55	45,45
49	Todos los procedimientos operativos identificados en la política de seguridad han de estar documentados	☐ FALSO	0			
50	Estan establecidas responsabilidades para controlar los cambios en equipos	☑ VERDADERO	1			
51	Estan establecidas responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad	☐ FALSO	0			
52	Existe algún método para reducir el mal uso accidental o deliberado de los	☐ FALSO	0			
53	Existe una separación de los entornos de desarrollo y producción	☐ FALSO	0			
54	Existen contratistas externos para la gestión de los Sistemas de Información	☑ VERDADERO	1			
55	Existe un Plan de Capacidad para asegurar la adecuada capacidad de proceso y de almacenamiento	☐ FALSO	0			
56	Existen criterios de aceptación de nuevos SI, incluyendo actualizaciones y nuevas versiones	☐ FALSO	0			
57	Controles contra software maligno	☑ VERDADERO	1			
58	Realizar copias de backup de la información esencial para el negocio	☐ FALSO	0			
59	Existen logs para las actividades realizadas por los operadores y administradores	☐ FALSO	0			
60	Existen logs de los fallos detectados	☐ FALSO	0			
61	Existen rastro de auditoría	☐ FALSO	0			
62	Existe algún control en las redes	☐ FALSO	0			
63	Hay establecidos controles para realizar la gestión de los medios informáticos.(cintas, discos, removibles, informes impresos)	☐ FALSO	0			
64	Eliminación de los medios informáticos. Pueden disponer de información	☐ FALSO	0			
65	Existe seguridad de la documentación de los Sistemas	☑ VERDADERO	1			
66	Existen acuerdos para intercambio de información y software	☐ FALSO	0			
67	Existen medidas de seguridad de los medios en el tránsito	☐ FALSO	0			
68	Existen medidas de seguridad en el comercio electrónico.	☐ FALSO	0			
69	Se han establecido e implantado medidas para proteger la confidencialidad e integridad de información publicada	☑ VERDADERO	1		si	no
70	Existen medidas de seguridad en las transacciones en linea	☑ VERDADERO	1			
71	Se monitorean las actividades relacionadas a la seguridad	☐ FALSO	0			
72	**CONTROL DE ACCESOS**		6		30,00	70,00
73	Existe una política de control de accesos	☐ FALSO	0			
74	Existe un procedimiento formal de registro y baja de accesos	☐ FALSO	0			
75	Se controla y restringe la asignación y uso de privilegios en entornos multi-usuario	☐ FALSO	0			
76	Existe una gestión de los password de usuarios	☐ FALSO	0			
77	Existe una revisión de los derechos de acceso de los usuarios	☐ FALSO	0			
78	Existe el uso del password	☑ VERDADERO	1			
79	Se protege el acceso de los equipos desatendidos	☐ FALSO	0			
80	Existen políticas de limpieza en el puesto de trabajo	☑ VERDADERO	1			
81	Existe una política de uso de los servicios de red	☐ FALSO	0			
82	Se asegura la ruta (path) desde el terminal al servicio	☑ VERDADERO	1			
83	Existe una autenticación de usuarios en conexiones externas	☑ VERDADERO	1			
84	Existe una autenticación de los nodos	☐ FALSO	0			
85	Existe un control de la conexión de redes	☐ FALSO	0			
86	Existe un control del routing de las redes	☐ FALSO	0			
87	Existe una identificación única de usuario y una automática de terminales	☐ FALSO	0			
88	Existen procedimientos de log-on al terminal	☐ FALSO	0			
89	Se ha incorporado medidas de seguridad a la computación móvil	☐ FALSO	0			
90	Está controlado el teletrabajo por la organización	☐ FALSO	0		si	no



	A	B	C	D	E	F
91	**DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS**		4		25,00	75,00
92	Se asegura que la seguridad está implantada en los Sistemas de Información	☑ VERDADERO	1			
93	Existe seguridad en las aplicaciones	☑ VERDADERO	1			
94	Existen controles criptográficos.	☐ FALSO	0			
95	Existe seguridad en los ficheros de los sistemas	☑ VERDADERO	1			
96	Existe seguridad en los procesos de desarrollo, testing y soporte	☑ VERDADERO	1		si	no
97	Existen controles de seguridad para los resultados de los sistemas	☐ FALSO	0			
98	Existe la gestión de los cambios en los SO.	☐ FALSO	0			
99	Se controlan las vulnerabilidades de los equipos	☐ FALSO	0			
100	**ADMINISTRACIÓN DE INCIDENTES**		4		50,00	50,00
101	Se comunican los eventos de seguridad	☐ FALSO	0			
102	Se comunican los debilidadesde seguridad	☐ FALSO	0			
103	Existe definidas las responsabilidades antes un incidente.	☐ FALSO	0			
104	Existe un procedimiento formal de respuesta	☐ FALSO	0			
105	Existe la gestión de incidentes	☐ FALSO	0			
106	**GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**		0		0,00	100,00
107	Existen procesos para la gestión de la continuidad.	☐ FALSO	0			
108	Existe un plan de continuidad del negocio y análisis de impacto	☐ FALSO	0			
109	Existe un diseño, redacción e implantación de planes de continuidad	☐ FALSO	0			
110	Existe un marco de planificación para la continuidad del negocio	☐ FALSO	0			
111	Existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio.	☐ FALSO	0		si	no
112	**CUMPLIMIENTO**		0		0,00	100,00
113	Se tiene en cuenta el cumplimiento con la legislación por parte de los sistemas	☐ FALSO	0			
114	Existe el resguardo de la propiedad intelectual	☐ FALSO	0			
115	Existe el resguardo de los registros de la organización	☑ VERDADERO	1			
116	Existe una revisión de la política de seguridad y de la conformidad técnica	☐ FALSO	0			
117	Existen consideraciones sobre las auditorías de los sistemas	☐ FALSO	0			
118			1		20,00	80,00

Anexo G. Diferencias entre COBIT® 5.0 y 4.1

COBIT® 5 incluye un modelo de referencia de procesos que define y describe en detalle varios procesos de gobierno y de gestión.

El modelo de procesos propuesto es completo, exhaustivo, pero no es el único modelo posible. Cada empresa debe definir su propio conjunto de procesos, teniendo en cuenta su situación específica.

El modelo de referencia de procesos de COBIT® 5 subdivide los procesos de gobierno y de gestión de TI de la empresa en dos principales áreas de actividad – gobierno y gestión – divididas en dominios de procesos:

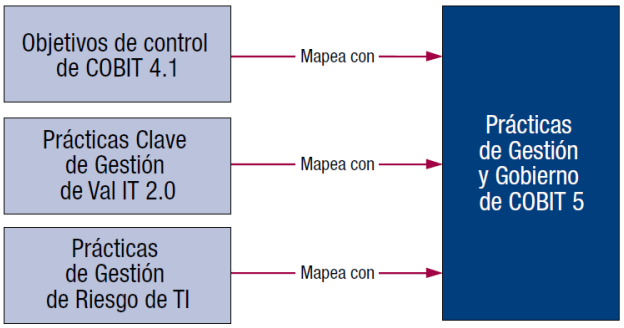
• Gobierno—Este dominio contiene cinco procesos de gobierno; dentro de cada proceso, se han definido las prácticas EDM.

• Gestión—Estos cuatro dominios están en línea con las áreas de responsabilidad de PBRM (una evolución de los dominios COBIT® 4.1), que proporcionan cobertura de TI extremo a extremo. Cada dominio contiene varios procesos, como en COBIT® 4.1 y versiones anteriores. Muchos de los procesos requieren actividades de 'planificación', 'implementación',' ejecución' y 'supervisión' del proceso o del caso específico acometido – p.ej., calidad, seguridad – estos son colocados en dominios en línea con lo que son generalmente las áreas de actividad más relevantes en cuanto al nivel TI de la empresa.

El modelo de referencia de proceso de COBIT® 5 es sucesor del modelo de proceso de COBIT® 4.1, con los modelos de proceso de Risk IT y Val IT también integrados.

En COBIT® 4.1, los controles del proceso contenían buenas prácticas que no eran específicas de ningún proceso, sino que eran genéricas y aplicables a todos los procesos.

Marcos de Trabajo de ISACA® incluidos en COBIT® 5.0



UNIVERSIDAD DE LA COSTA 1970	NORMAS PARA LA ENTREGA DE TESIS Y TRABAJOS DE GRADO A LA UNIDAD DE INFORMACION	VERSION: 02 FECHA: Junio 2012 CODIGO:DOC-VACRE-NETGUDI

CARTA DE ENTREGA Y AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCIÓN PARCIAL O TOTAL, Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO DE TESIS Y TRABAJOS DE GRADO

Barranquilla, Octubre 31 de 2014

Marque con una X
Tesis [ ] **Trabajo de Grado** [X]

Yo, Ana Maria Molinares Donado, identificada con C.C. No. 22.479.853, actuando en nombre propio y como autora de la tesis y/o trabajo de grado titulado: CONSULTORÍA APLICADA AL PROCESO DE TECNOLOGÍA DE LA INFORMACIÓN DE LA EMPRESA CONGLOMERADO TÉCNICO COLOMBIANO S.A. – CONTECSA S.A, presentado y aprobado en el año 2.014 como requisito para optar al título de Especialista en Auditoria a los Sistemas de Información; hago entrega del ejemplar respectivo y de sus anexos de ser el caso, en formato digital o electrónico (DVD) y autorizo a la UNIVERSIDAD DE LA COSTA, CUC, para que en los términos establecidos en la Ley 23 de 1982, Ley 44 de 1993, Decisión Andina 351 de 1993, Decreto 460 de 1995 y demás normas generales sobre la materia, utilice y use en todas sus formas, los derechos patrimoniales de reproducción, comunicación pública, transformación y distribución (alquiler, préstamo público e importación) que me corresponden como creador de la obra objeto del presente documento.

Y autorizo a la Unidad de información, para que con fines académicos, muestre al mundo la producción intelectual de la Universidad de la Costa, CUC, a través de la visibilidad de su contenido de la siguiente manera:

Los usuarios puedan consultar el contenido de este trabajo de grado en la página Web de la Facultad, de la Unidad de información, en el repositorio institucional y en las redes de información del país y del exterior, con las cuales tenga convenio la institución y Permita la consulta, la reproducción, a los usuarios interesados en el contenido de este trabajo, para todos los usos que tengan finalidad académica, ya sea en formato DVD o digital desde Internet, Intranet, etc., y en general para cualquier formato conocido o por conocer.

El AUTOR - ESTUDIANTE, manifiesta que la obra objeto de la presente autorización es original y la realizó sin violar o usurpar derechos de autor de terceros, por lo tanto la obra es de su exclusiva autoría y detenta la titularidad ante la misma. PARÁGRAFO: En caso de presentarse cualquier reclamación o acción por parte de un tercero en cuanto a los derechos de autor sobre la obra en cuestión, EL ESTUDIANTE - AUTOR, asumirá toda la responsabilidad, y saldrá en defensa de los derechos aquí autorizados; para todos los efectos, la Universidad actúa como un tercero de buena fe.

Para constancia se firma el presente documento en dos (02) ejemplares del mismo valor y tenor, en Barranquilla D.E.I.P., a los 31 días del mes de Octubre de Dos Mil Catorce.

ANA MARIA MOLINARES DONADO

UNIVERSIDAD DE LA COSTA CUC 1970	NORMAS PARA LA ENTREGA DE TESIS Y TRABAJOS DE GRADO A LA UNIDAD DE INFORMACION	VERSION: 02 FECHA: Junio 2012 CODIGO:DOC-VACRE-NETGUDI

CARTA DE ENTREGA Y AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCIÓN PARCIAL O TOTAL, Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO DE TESIS Y TRABAJOS DE GRADO

Barranquilla, Octubre 31 de 2014

Marque con una X
Tesis [ ] **Trabajo de Grado** [X]

Yo, Lenys Rangel Ferrer, identificada con C.C. No. 55.230.510, actuando en nombre propio y como autora de la tesis y/o trabajo de grado titulado: CONSULTORÍA APLICADA AL PROCESO DE TECNOLOGÍA DE LA INFORMACIÓN DE LA EMPRESA CONGLOMERADO TÉCNICO COLOMBIANO S.A. – CONTECSA S.A, presentado y aprobado en el año 2.014 como requisito para optar al título de Especialista en Auditoria a los Sistemas de Información; hago entrega del ejemplar respectivo y de sus anexos de ser el caso, en formato digital o electrónico (DVD) y autorizo a la UNIVERSIDAD DE LA COSTA, CUC, para que en los términos establecidos en la Ley 23 de 1982, Ley 44 de 1993, Decisión Andina 351 de 1993, Decreto 460 de 1995 y demás normas generales sobre la materia, utilice y use en todas sus formas, los derechos patrimoniales de reproducción, comunicación pública, transformación y distribución (alquiler, préstamo público e importación) que me corresponden como creador de la obra objeto del presente documento.

Y autorizo a la Unidad de información, para que con fines académicos, muestre al mundo la producción intelectual de la Universidad de la Costa, CUC, a través de la visibilidad de su contenido de la siguiente manera:

Los usuarios puedan consultar el contenido de este trabajo de grado en la página Web de la Facultad, de la Unidad de información, en el repositorio institucional y en las redes de información del país y del exterior, con las cuales tenga convenio la institución y Permita la consulta, la reproducción, a los usuarios interesados en el contenido de este trabajo, para todos los usos que tengan finalidad académica, ya sea en formato DVD o digital desde Internet, Intranet, etc., y en general para cualquier formato conocido o por conocer.

El AUTOR - ESTUDIANTE, manifiesta que la obra objeto de la presente autorización es original y la realizó sin violar o usurpar derechos de autor de terceros, por lo tanto la obra es de su exclusiva autoría y detenta la titularidad ante la misma. PARÁGRAFO: En caso de presentarse cualquier reclamación o acción por parte de un tercero en cuanto a los derechos de autor sobre la obra en cuestión, EL ESTUDIANTE - AUTOR, asumirá toda la responsabilidad, y saldrá en defensa de los derechos aquí autorizados; para todos los efectos, la Universidad actúa como un tercero de buena fe.

Para constancia se firma el presente documento en dos (02) ejemplares del mismo valor y tenor, en Barranquilla D.E.I.P., a los 31 días del mes de Octubre de Dos Mil Catorce.

LENYS RANGEL FERRER

UNIVERSIDAD DE LA COSTA CUC 1970	NORMAS PARA LA ENTREGA DE TESIS Y TRABAJOS DE GRADO A LA UNIDAD DE INFORMACION	VERSION: 02 FECHA: Junio 2012 CODIGO:DOC-VACRE-NETGUDI

CARTA DE ENTREGA Y AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCIÓN PARCIAL O TOTAL, Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO DE TESIS Y TRABAJOS DE GRADO

Barranquilla, Octubre 31 de 2014

Marque con una X
Tesis [ ] **Trabajo de Grado** [X]

Yo, Manuela Maria Villar Ávila, identificada con C.C. No. 1.045.671.412, actuando en nombre propio y como autora de la tesis y/o trabajo de grado titulado: CONSULTORÍA APLICADA AL PROCESO DE TECNOLOGÍA DE LA INFORMACIÓN DE LA EMPRESA CONGLOMERADO TÉCNICO COLOMBIANO S.A. – CONTECSA S.A, presentado y aprobado en el año 2.014 como requisito para optar al título de Especialista en Auditoria a los Sistemas de Información; hago entrega del ejemplar respectivo y de sus anexos de ser el caso, en formato digital o electrónico (DVD) y autorizo a la UNIVERSIDAD DE LA COSTA, CUC, para que en los términos establecidos en la Ley 23 de 1982, Ley 44 de 1993, Decisión Andina 351 de 1993, Decreto 460 de 1995 y demás normas generales sobre la materia, utilice y use en todas sus formas, los derechos patrimoniales de reproducción, comunicación pública, transformación y distribución (alquiler, préstamo público e importación) que me corresponden como creador de la obra objeto del presente documento.

Y autorizo a la Unidad de información, para que con fines académicos, muestre al mundo la producción intelectual de la Universidad de la Costa, CUC, a través de la visibilidad de su contenido de la siguiente manera:

Los usuarios puedan consultar el contenido de este trabajo de grado en la página Web de la Facultad, de la Unidad de información, en el repositorio institucional y en las redes de información del país y del exterior, con las cuales tenga convenio la institución y Permita la consulta, la reproducción, a los usuarios interesados en el contenido de este trabajo, para todos los usos que tengan finalidad académica, ya sea en formato DVD o digital desde Internet, Intranet, etc., y en general para cualquier formato conocido o por conocer.

El AUTOR - ESTUDIANTE, manifiesta que la obra objeto de la presente autorización es original y la realizó sin violar o usurpar derechos de autor de terceros, por lo tanto la obra es de su exclusiva autoría y detenta la titularidad ante la misma. PARÁGRAFO: En caso de presentarse cualquier reclamación o acción por parte de un tercero en cuanto a los derechos de autor sobre la obra en cuestión, EL ESTUDIANTE - AUTOR, asumirá toda la responsabilidad, y saldrá en defensa de los derechos aquí autorizados; para todos los efectos, la Universidad actúa como un tercero de buena fe.

Para constancia se firma el presente documento en dos (02) ejemplares del mismo valor y tenor, en Barranquilla D.E.I.P., a los 31 días del mes de Octubre de Dos Mil Catorce.

MANUELA MARIA VILLAR ÁVILA

UNIVERSIDAD DE LA COSTA	**NORMAS PARA LA ENTREGA DE TESIS Y TRABAJOS DE GRADO A LA UNIDAD DE INFORMACION**	**VERSION: 02** **FECHA: Junio 2012** **CODIGO:DOC-VACRE-NETGUDI**

FORMULARIO DE LA DESCRIPCIÓN DE LA TESIS O DEL TRABAJO DE GRADO

TÍTULO COMPLETO DE LA TESIS O TRABAJO DE GRADO:

CONSULTORÍA APLICADA AL PROCESO DE TECNOLOGÍA DE LA INFORMACIÓN DE LA EMPRESA CONGLOMERADO TÉCNICO COLOMBIANO S.A. – CONTECSA S.A.

SUBTÍTULO, SI LO TIENE:

_____

_____

AUTOR AUTORES

Apellidos Completos	Nombres Completos
Molinares Donado Rangel Ferrer Villar Ávila	Ana Maria Lenys Manuela Maria

DIRECTOR (ES)

Apellidos Completos	Nombres Completos
Montaño Ardila	Víctor Manuel

JURADO (S)

Apellidos Completos	Nombres Completos
Martínez Palacio De La Hoz Franco	Ubaldo Emiro

ASESOR (ES) O CODIRECTOR

Apellidos Completos	Nombres Completos
Barraza Olaya	Telma Leticia

TRABAJO PARA OPTAR AL TÍTULO DE: Especialista en Auditoria a los Sistemas de Información

FACULTAD: _____

PROGRAMA: Pregrado _____ Especialización X

NOMBRE DEL PROGRAMA_____

UNIVERSIDAD DE LA COSTA 1970	**NORMAS PARA LA ENTREGA DE TESIS Y TRABAJOS DE GRADO A LA UNIDAD DE INFORMACION**	**VERSION: 02** **FECHA: Junio 2012** **CODIGO:DOC-VACRE-NETGUDI**

CIUDAD: Barranquilla AÑO DE PRESENTACIÓN DEL TRABAJO DE GRADO: 2014

NÚMERO DE PÁGINAS 111

TIPO DE ILUSTRACIONES:

- [ ] Ilustraciones
- [ ] Láminas
- [ ] Retratos
- [x] Tablas, gráficos y diagramas
- [ ] Planos
- [ ] Mapas
- [ ] Fotografías

MATERIAL ANEXO (Vídeo, audio, multimedia o producción electrónica): Duración del audiovisual: __minutos.

Número de casetes de vídeo: _____ Formato: VHS ___Beta Max _¾ _Beta Cam _____

Mini DV _____DV Cam _____ DVC Pro ____Vídeo 8 _____ Hi 8 ____

Otro. Cuál? _____

Sistema: Americano NTSC _____Europeo PAL _____ SECAM _____

Número de casetes de audio: _____

Número de archivos dentro del DVD (En caso de incluirse un DVD diferente al trabajo de grado):

_____

PREMIO O DISTINCIÓN *(En caso de ser LAUREADAS o tener una mención especial)*:

_____

DESCRIPTORES O PALABRAS CLAVES EN ESPAÑOL E INGLÉS: Son los términos que definen los temas que identifican el contenido. (*En caso de duda para designar estos descriptores, se recomienda consultar con la Unidad de Procesos Técnicos de la Unidad de información en el correo biblioteca@cuc.edu.co, donde se les orientará).*

ESPAÑOL	**INGLÉS**
_____	_____
_____	_____
_____	_____

RESUMEN DEL CONTENIDO EN ESPAÑOL E INGLÉS:(Máximo 250 palabras-1530 caracteres):

_____

_____

_____